https://lajc.epn.edu.ec

ESCUELA POLITÉCNICA NACIONAL

Facultad de Ingeniería de Sistemas

VOLUME 9, ISSUE 2
JULY 2022
ISSN: 1390-9266
e-ISSN:1390-9134

LATIN-AMERICAN JOURNAL OF COMPUTING

Associated Institutions:

UDLA

UTA Universidad Técnica de Ambato

UDEM

UPR Recinto Universitario de Mayagüez

Vol IX, Issue 2, July 2022

ESCUELA
POLITÉCNICA
NACIONAL

https://www.epn.edu.ec

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

MISIÓN

La Escuela Politécnica Nacional es una Universidad pública, laica y democrática que garantiza la libertad de pensamiento de todos sus integrantes, quienes están comprometidos con aportar de manera significativa al progreso del Ecuador. Formamos investigadores y profesionales en ingeniería, ciencias, ciencias administrativas y tecnología, capaces de contribuir al bienestar de la sociedad a través de la difusión del conocimiento científico que generamos en nuestros programas de grado, posgrado y proyectos de investigación. Contamos con una planta docente calificada, estudiantes capaces y personal de apoyo necesario para responder a las demandas de la sociedad ecuatoriana.

VISIÓN

En el 2024, la Escuela Politécnica Nacional es una de las mejores universidades de Latinoamérica con proyección internacional, reconocida como un actor activo y estratégico en el progreso del Ecuador. Forma profesionales emprendedores en carreras y programas académicos de calidad, capaces de aportar al desarrollo del país, así como promover y adaptarse al cambio y al desarrollo tecnológico global. Posiciona en la comunidad científica internacional a sus grupos de investigación y provee soluciones tecnológicas oportunas e innovadoras a los problemas de la sociedad.

La comunidad politécnica se destaca por su cultura de excelencia y dinamismo al servicio del país dentro de un ambiente de trabajo seguro, creativo y productivo, con infraestructura de primer orden.

ACCIÓN AFIRMATIVA

La Escuela Politécnica Nacional es una institución laica y democrática, que garantizar la libertad de pensamiento, expresión y culto de todos sus integrantes, sin discriminación alguna. Garantiza y promueve el reconocimiento y respeto de la autonomía universitaria, a través de la vigencia efectiva de la libertad de cátedra y de investigación y del régimen de cogobierno.

FACULTAD DE INGENIERÍA DE SISTEMAS

https://fis.epn.edu.ec

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

MISIÓN

La Facultad de Ingeniería de Sistemas es el referente de la Escuela Politécnica Nacional en el campo de conocimiento y aplicación de las Tecnologías de Información y Comunicaciones; actualiza en forma continua y pertinente la oferta académica en los niveles de pregrado y postgrado para lograr una formación de calidad, ética y solidaria; desarrolla proyectos de investigación, vinculación y proyección social en su área científica y tecnológica para solucionar problemas de transcendencia para la sociedad.

VISIÓN

La Facultad de Ingeniería de Sistemas está presente en posiciones relevantes de acreditación a nivel nacional e internacional y es referente de la Escuela Politécnica Nacional en el campo de las Tecnologías de la Información y Comunicaciones por su aporte de excelencia en las carreras de pregrado y postgrado que auspicia, la calidad y cantidad de proyectos de investigación, vinculación y proyección social que desarrolla y su aporte en la solución de problemas nacionales a través del uso intensivo y extensivo de la ciencia y la tecnología.

LATIN-AMERICAN JOURNAL OF COMPUTING

Vol IX, Issue 2, July 2022

ISSN: 1390-9266 e-ISSN: 1390-9134

Published by:
Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas

Quito – Ecuador

Mailing Address

Escuela Politécnica Nacional,
Facultad de Ingeniería de Sistemas
Ladrón de Guevara E11-253, La Floresta
Quito-Ecuador, Apartado Postal: 17-01-2759

Web Address

https://lajc.epn.edu.ec/

E-mail

lajc@epn.edu.ec

Frequency

2 issues per year

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

Published by

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas
Ecuador

Editor in Chief

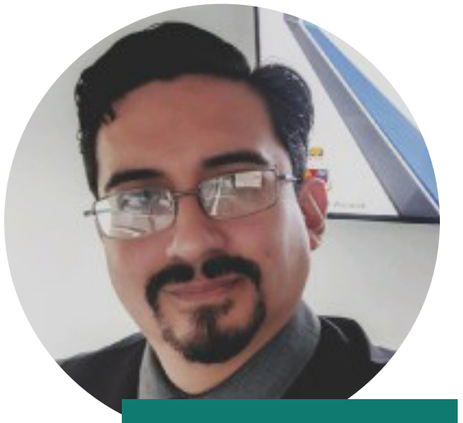
Editorial Committee

Co-Editors

Assistant Editors

Proofreader

EDITORIAL



Denys A. Flores. PhD.

Editor in Chief
Escuela Politécnica Nacional, Ecuador

Ideas abiertas, conocimiento libre.

La divulgación de la ciencia, más que una oportunidad, debe ser vista como un derecho de todos para mejorar nuestra sociedad a través de las ideas. Sin embargo, los costos de publicación excesivos y las prácticas depredadoras han empañado las posibilidades para que los investigadores difundan sus pensamientos a audiencias más amplias. Las publicaciones de Acceso Abierto fueron concebidas para equilibrar estas desigualdades, y la Revista Latinoamericana de Computación (LAJC) no es una excepción.

Durante el primer semestre de 2022, nuestro Comité Editorial, comprometido con el libre acceso a la ciencia y la tecnología, ha trabajado arduamente para ofrecer mejores oportunidades de publicación gratuitas y atractivas a investigadores de todo el mundo. Nuestro alcance se reestructuró para cubrir más áreas en el campo de la computación y la informática, y nuestra base de datos de revisores se amplió para maximizar la calidad de la retroalimentación que ofrecemos a todos nuestros potenciales autores. Como resultado, seguimos avanzando en la internacionalización de nuestra Revista, presentándoles en este número interesantes artículos de investigadores de Ecuador, Colombia, Argentina, Alemania y el Reino Unido.

Comenzamos con un análisis de ciber amenazas en centrales eléctricas virtuales en el que se utiliza un método heurístico para evaluarlas, considerando su impacto en la estabilidad y confiabilidad de una red eléctrica. En el campo de la informática forense, se analizan métodos para eludir la autenticación de usuario, reduciendo la posible pérdida de evidencia cuando una computadora está bloqueada y se desconocen las credenciales de acceso. Con respecto a métodos mejorados de seguridad informática, se evalúan los sensores de los teléfonos móviles para obtener una mayor precisión cuando se utilizan para la autenticación de usuarios. Se utiliza una red neuronal feed-forward para evaluar la discriminabilidad, la estabilidad y la confiabilidad de los sensores para autenticación activa y continua. En cuanto a e-democracia, se presenta un sistema de voto electrónico que utiliza un esquema de firma ciega para garantizar la privacidad de los usuarios y la seguridad de los votos.

Finalmente, LAJC es una de las pocas revistas que da la bienvenida a resultados preliminares de investigación. En este número, se presenta una revisión literaria sobre técnicas para la enseñanza de la lectura de labios a personas sordas que examina trabajos recientes, combinando metodologías de aprendizaje y tecnología. Además, se describe el proceso de ingeniería de una agenda personal para personas ciegas. Esta propuesta llena el vacío existente en las aplicaciones móviles que normalmente no están diseñadas para personas con discapacidad visual, marcando el camino para el desarrollo de soluciones más inclusivas utilizando la informática.

Invitamos amablemente a nuestra audiencia a leer este número que muestra nuestros esfuerzos para aumentar el alcance de la investigación de acceso abierto, así como nuestra incansable voluntad de maximizar el impacto del trabajo desarrollado por nuestros autores, independientemente de su ubicación geográfica.

Estamos humildemente orgullosos de lo que hemos logrado hasta ahora, manteniendo la mirada fija en un horizonte optimista. Reafirmamos nuestro compromiso de hacer de LAJC, un recipiente gratuito para vuestras ideas.

Gracias por su apoyo constante.

Denys A. Flores.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762873

Open ideas, free knowledge.

The dissemination of science, more than an opportunity, should be seen as a right for everyone to improve our society through ideas. However, excessive publication costs and predatory practices have tarnished the chances for researchers to spread their thoughts to broader audiences. Open Access publications were conceived to balance these inequities, and the Latin-American Journal of Computing (LAJC) is not an exception.

During the first semester of 2022, our Editorial Board, committed with free access to science and technology, has worked hard to offer better, free, and attractive publication opportunities to researchers worldwide. Our scope was re-structured to cover more areas in the field of computing and informatics, and our reviewer database was expanded accordingly to maximize the feedback quality that we offer to all our prospective authors. As a result, we keep moving forward towards the internationalization of our Journal, introducing in this issue interesting articles of researchers from Ecuador, Colombia, Argentina, Germany, and the United Kingdom.

We begin with an analysis of cyberthreats in virtual power plants in which a heuristic method to evaluate them is used, considering their impact in the stability and reliability of a power grid. In the field of computer forensics, methods to bypass user authentication are analyzed, reducing potential evidence loss when a computer is locked, and access credentials are unknown. Regarding enhanced methods of computer security, mobile phone sensors are evaluated for better accuracy when used for user authentication. A feed-forward neural network is used for evaluating sensors' discriminability, stability, and reliability for active and continuous authentication. Concerning e-democracy, an e-voting system is presented using a blind signature scheme to guarantee users' privacy and security of votes.

Finally, LAJC is one of the few journals that welcomes early research results. In this issue, a literature review of techniques for lip-reading teaching to deaf people is presented, which examines recent work combining learning methodologies and technology. Also, the engineering process to develop a personal agenda for blind people is described. This proposal fills the gap in existing mobile applications which are typically not designed for people with visual impairment, paving the road for developing more inclusive solutions using informatics.

Our audience is kindly invited to read this issue which showcase our efforts to increase the outreach of open access research, and our relentless will to maximize the impact of the work developed by our authors, regardless their geographical location.

We are humbly proud of what we have achieved so far, keeping our eyes fixed in an optimistic horizon. We reaffirm our commitment to make LAJC, a free-of-charge vessel for your ideas.

Thank you for your constant support.

Denys A. Flores.

LATIN-AMERICAN JOURNAL OF COMPUTING

We are most grateful to the following individuals for their time and commitment to review manuscripts for the Latin American Journal of Computing – LAJC

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

Reviewers

Carlos Anchundia, MSc.
Escuela Politécnica Nacional

Carlos Montenegro, MSc.
Escuela Politécnica Nacional

Cesar Salinas, MSc.
Universidad de las Américas

David Nuñez, MSc.
CNT EP

Diego Almeida, PhD.
School of Biological Sciences and Engineering, Universidad Yachay Tech

Diego Riofrío, PhD.
Universidad Internacional SEK

Edison Loza, PhD.
Escuela Politécnica Nacional

Edward Chuah, PhD.
The University of Exeter, UK

Evelyn Del Pezo, PhD.
Universidad de Guayaquil

Fernando Molina, PhD.
Universidad Nacional de Chimborazo

Freddy Tapia, PhD.
Universidad de las Fuerzas Armadas

Henry Paz, MSc.
Escuela Politécnica Nacional

Jenny Torres, PhD.
Escuela Politécnica Nacional

Jessica Morales, MSc.
ESPAM MFL, Grupo de Investigación SISCOM

Jhonattan Barriga, MSc.
Escuela Politécnica Nacional

Jorge Zambrano, PhD.
Universitat Politécnica de Valéncia

José Lucio, PhD.
Escuela Politécnica Nacional

Juan Herrera, MSc.
Escuela Politécnica Nacional

Julián Galindo, PhD.
Escuela Politécnica Nacional

Katty Rohoden, MSc.
Universidad Técnica Particular de Loja

Lenin Falconi, MSc.
Fiscalía General del Estado

Leonardo Valdivieso, PhD.
Escuela Politécnica Nacional

Lorena Recalde, PhD.
Escuela Politécnica Nacional

Marcela Mosquera, MSc.
Escuela Politécnica Nacional

Marco Benalcázar, PhD.
Escuela Politécnica Nacional

Marco Galarza, MSc.
Universidad de las Américas

Marco Santórum, PhD.
Escuela Politécnica Nacional

María Pérez, PhD.
Escuela Politécnica Nacional

Mirian Peñafiel, PhD.
Escuela Politécnica Nacional

Monserrate Intriago, MSc.
Escuela Politécnica Nacional

Pablo del Hierro, PhD.
Escuela Politécnica Nacional

Roberto Andrade, MSc.
Escuela Politécnica Nacional

Rosa Navarrete, PhD.
Escuela Politécnica Nacional

Sang Yoo, PhD.
Escuela Politécnica Nacional

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

TABLE OF CONTENTS

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

Assessing the Cyber Threat Landscape for Virtual Power Plants

ARTICLE HISTORY

Received 10 March 2022
Accepted 02 May 2022

George Gkoktsis
Cyber-Physical Systems Security
Fraunhofer SIT
Darmstadt, Germany
george.gkoktsis@sit.fraunhofer.de

"Assessing the Cyber Threat Landscape for Virtual Power Plants",
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.
G. Gkoktsis,

Assessing the Cyber Threat Landscape for Virtual Power Plants

George Gkoktsis
Cyber-Physical Systems Security
Fraunhofer SIT
Darmstadt – Germany
george.gkoktsisgvidal@sit.fraunhofer.de

Abstract— Virtual Power Plants (VPPs) aggregate and coordinate Distributed Energy Resources (DER) as a single entity aiding in the decarbonization of the energy generation mix. The infrastructure of VPPs relies heavily on the rigorous and accurate exchange of information between the DER and the VPP, as well as other grid entities. This exposes them to possible cyber threats that impede their functions and can have negative impacts on the stability and reliability of the grid. This paper evaluates the threat landscape against threats that affect VPPs. A heuristic method of assessing the impact and likelihood of attacks is constructed based on a) proposed methods in the literature, b) standardization bodies, and c) in relation to a VPPs security profile. Our findings indicate that False Data Injection attacks pose the greatest risk, competing with disruption of their functions due to Denial of Service.

Keywords— *Virtual Power Plants, Cyber-Physical Security, Smart Grid Security*

I. INTRODUCTION

Renewable generation is promoted as decarbonization plans are followed through all over the globe in an effort to reduce CO2 emissions. Renewables are constructed where their potential is harnessed, for example, wind generators are installed on mountaintops or offshore. They are referred to as Distributed Energy Resources (DER). Energy dispatch scheduling is performed based on load curve forecasts. Periodically, daily, monthly etc., the expected consumption is calculated, and generation is scheduled accordingly to satisfy the load. DER have small generation capacity in general, 2-3 orders of magnitude smaller than fuel-based generators and are numerous. Thus, including them in dispatch scheduling individually is mostly inefficient. Their very fast connection to the grid capability, however, enables them to participate in demand response, i.e., the dynamic grid generation and load management. Due to these reasons, Virtual Power Plants (VPPs) are created to aggregate DER generation, optimize control, and interact with the market in a coordinated and profitable manner.

There are many definitions in the literature about VPPs. This paper defines a VPP as: "A portfolio of DERs, which are connected by a control system based on information and communication technology (ICT). The VPP acts as a single visible entity in the power system, is always grid-tied and can be either static or dynamic" [1]. In the Smart Grid Architecture Model [2]Integrity and Availability, VPPs are loosely described as "aggregation of DER". However, they have the potential to substantial aggregate amounts of generation capacity, reaching GW of output, and thus comparable to Steam units so they can be considered critical infrastructure.

In the absence of standardized architectures, implementations of VPPs are based on the vision of individual organizations, where software solutions are used to control and dispatch DER. The "control system" aspect of the definition is usually an amalgamation of interoperable firmware and proprietary software capable of interfacing the VPP management platform and responding to market signals. Moreover, due to the topological distribution of participating generation, it is hard, if not impossible, for critical communication channels to avoid being implemented over the wider internet.

Energy systems are engineered to provide safe, reliable, and robust energy generation and delivery. Cyber threats against them can cause instabilities, which can lead to instigation of cascading failure events [3], [4]. Attackers may exploit weaknesses in the architecture to cause blackouts [5] or invalidate safety equipment [6].

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

An additional difficulty in VPP cybersecurity is the plurality of stakeholders participating in the structure. The VPP operator may not be the owner of the DER but act only as a mediator between generating entities and the energy market. DER are electrically connected to Distribution System Operator's (DSO) infrastructure. Jurisdiction and liability for security policy creation and enforcement are not trivial in an environment rich with cyber-physical dependencies between different legal entities. The dependence on third-party assurances in the form of trustworthy software and hardware complicates further the situation. For example, a smart inverter operating on third party software can be attacked [7]converting electric power and energy into several forms and magnitudes. Power electronics also facilitate the control of distributed generation and storage assets. Inverters are prominent power electronics found in many customer premises because of their pertinence in converting electricity from DC to AC. Smart inverters go beyond basic conversion and have the potential to support the utility system. The additional grid support function creates some cyber security vulnerabilities, especially when the grid relies on inverter-dependent DER in high proliferation areas. In California., the Smart Inverter Working Group (SIWG by exploiting a design flaw in the software. Changing the settings will affect the power output of the DER, possibly creating system instability in the process. This affects both the VPP, as well as the general grid. It may be challenging to determine who bears responsibility for securing the infrastructure and who is liable for the damages.

Assessing the threat landscape for VPPs is of vital importance for most of their cyber security activities. For security management, it enables accurate estimation of risk [8]. It assists threat modelling in identifying the threat actors that need to be tracked, as a result augmenting detection of their activities. Then, response and remediation plans and playbooks can be designed and implemented, supporting cyber resilience. The field is relatively immature, and, in our opinion, it is important to take the physical system into consideration while performing this exercise.

To avoid the aforementioned complications and in an effort to preserve the generality principle, in this paper, a VPP is abstracted to three functions that must be fulfilled, as per the accepted definition, and the threat landscape is assessed against any adversarial effort to invalidate these functions. They are:

1. Interaction with the energy market and demand response,
2. Supervision and control of participating DER,
3. Safe operation of DER.

This paper aims to contribute in the following ways: i) illuminate the unique security threats and requirements of VPPs, and ii) propose a heuristic impact and likelihood evaluation method within the scope and definitions of VPPs.

II. RELATED WORK

In this section, an overview of relevant research to smart grid threat landscape and VPP security is presented. First, the threat landscape itself is presented and then research specific to VPP cybersecurity.

In [9], the European Union Agency for Cybersecurity (ENISA) presents the cyber threats related to the smart grid while taking into consideration possible physical attacks that may be relevant. The necessity for developing threat intelligence in the form of attack scenarios is showcased, as well as the gap in the criticality assessment of smart grid assets and processes. Considering the rapidly evolving threat environment for critical infrastructures, it would be considered outdated.

The National Electric Sector Cybersecurity Organization Resource (NESCOR) described a plethora of attack scenarios against the smart grid in [10], [11], organized into 6 categories. Two of those are closely relevant to VPPs, namely DER and Wide Area Monitoring, Protection and Control (WAMPAC). Amongst others, a threat model and 16 threat impact evaluation criteria are being presented to facilitate a risk representation of scenarios tailor-made for the smart grid. In order to generate threat intelligence, these scenarios need to be tested, and use cases constructed, as attempted in various research efforts, like [12]–[14]. To our knowledge, no use case was constructed for VPP structures.

Within the CYBER-TRUST project [15], a threat landscape for Trusted Internet of Things was constructed, with a section devoted solely to threats against the smart grid. The alleviating effect of our state-of-the-art security practices, like the presence of firewalls, IPS, anti-malware, the existence of security policies etc., is then estimated. However, according to their analysis, these countermeasures have little to no effect on mitigating the smart grid-specific threats. Considering the characteristics of VPPs, this problem is further exacerbated by the fact that critical communications can be utilized in home-area networks, wired or wireless, which are intrinsically unsafe.

In [16], Sandia National presents a design and evaluation of secure VPPs. While taking into consideration all aforementioned hurdles, the viability of signal correlations for Intrusion Detection Systems is showcased, and a network segmentation strategy, which is performed with topological-operational considerations, is suggested. Attacks are simulated in PowerWorld, and the system's response is then correlated with attack-free conditions. The attack scenarios themselves involve malicious disconnections of VPP elements and malicious generation manipulation, like ramping up/down active/reactive power output of DER. For our paradigm, these scenarios only address the third function of a VPP, the safe operation of DER. Their adversarial model assumes one action of the attacker, which is also a limiting factor. Additionally, it is unclear whether the effects can be uniquely caused by adversarial activity or due to faulty operation.

Hussain et al. [17] explain the adoption of the IEC 62351 standard for IEC 61850 communication channels. Its relevance to VPPs lies in the analysis of routable IEC 61850 protocols for DER coordination, like IEC 60870-104 and derivatives, R-GOOSE and R-SV, and MMS. Even though IEC 62351 is an improvement of the inherent weaknesses of R-GOOSE and R-SV, Quality of Service requirements limits the applicable integrity and source authentication mechanisms to the use of HMACs, without consideration of confidentiality. However, when routed over untrusted networks, confidentiality becomes a requirement, as the messages may contain sensitive information, such as the financial information of the DER. Furthermore, authentication of DER equipment has embedded certificates for Digital Signature schemes, which are hard coded in the Intelligent Electrical Devices (IEDs) and lack the ability to be revoked when compromised.

III. THREAT EVALUATION CRITERIA

This section presents the methodology employed for threat assessment. Each threat was examined towards its relevance to the security profile of a VPP. A qualitative assessment of the impact by adapting the NESCOR impact evaluation scales, was performed. Similarly, the likelihood assessment adapted the relevant scales while taking into consideration published literature and vulnerability databases. The scoring of each criterion is also influenced by CEN-CELEC-ETSI and NIST recommendations.

A. VPP CYBERSECURITY PROFILE

The US National Institute of Standards and Technology (NIST), in their Technical Note 2051 [18], introduces the cybersecurity profile for the Smart Grid. It assists with cybersecurity management of organizations participating in the energy infrastructure with heavy penetration of DER and consists of five high-level security categories, namely: Identify, Protect, Detect, Respond, Recover. These consist of 108 subcategories such as Asset Management, Risk Assessment, Identity Management, Access Control etc. Together they form the Core of a Cybersecurity profile. Business objectives, cybersecurity requirements and the technical environment is given as an input to the profile, and operating methodologies are the output.

In order to form a basis for the threat assessment for VPPs, a high-level security profile for them was created. It was used as a tool to examine the relevance of a particular threat to the high-level security objectives of VPPs. Fig. 1 shows a diagram of the process used to create the VPP profile. In Step 1, the operational functions of the VPP are defined as business mission objectives. Thus, sets of the core functions are created for every objective.

Eventhough the maintenance of safety, reliability, resilience, and support for grid modernization is described as business objectives in the Technical Note, we opted to input them to the profile as requirements, as there are legal requirements for their maintenance when part of the critical infrastructure. This is given as input to the core of the profile in Step 2. At the end of Step 2, for every mission objective, the security requirements are deduced.

Step 3 is the threat modelling part of the process. Here, the threat landscape is mapped to each business objective and classified per security requirement. Security gaps, like protocol weaknesses, or possible legacy equipment, are also taken into consideration as system vulnerabilities and are mapped alongside the known threats. For example, an adversary attempting to alter the power setpoint of a DER threatens the reliability requirement of the secure DER operation objective. The threat is examined on how the threat should be identified, responded to, and mitigated. Failure to do so produces the impacts that are then evaluated by the assessment criteria.

The output of the profile is the mitigations of each threat based on the aforementioned analysis. These can be either technical controls or policies, depending on the function that is invalidated. In the above example, source authentication and access management policy creation are possible countermeasures. In this paper, however, this part is omitted, as a resilient response to attacks and disturbances for VPPs is a future goal of our research.

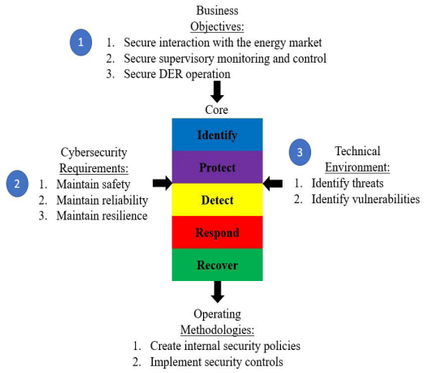


Fig. 1 Security Profile of a VPP creation process

B. IMPACT ASSESSMENT CRITERIA

To estimate the effects of successful attacks, we adapted and scaled the NESCOR impact criteria [10] to fit the VPP paradigm, summarized in Table I.

The final impact score of an attack was calculated as the mean average of the score of each criterion. A more precise approach would be to calculate a weighted average of the scores, as they scale at different rates, and their relative value is difficult to quantify. Specifically, the safety ranking and the ecological concerns (which are omitted in this analysis, as VPPs are mostly comprised of DER and generation is assumed to not involve chemical, radioactive, or kinetic processes), are problematic as in this evaluation, the loss of human life is of equal importance as the instigation of system instabilities. The exercise of accurately quantifying them, however, is out of scope of this research.

To mitigate this imbalance, two additional rules were used. If a threat is scored 9 at the safety criterion, it is automatically considered critical, regardless of other scores. If a threat scores 9 in at least two other categories, it is considered critical.

TABLE I. Impact Assessment Criteria

Criterion	Scoring	
	Minimum Score	Maximum Score
System scale	0: single DER affected	9: All DER affected
Safety	0: none	9: 1 possible death
Financial Impact on VPP	0: petty cash	9: >5% of revenue
Negative impact on generation capacity	0: none	9: >10% for more than 8 hours
Negative impact on the energy market	0: None	9: Loss of market participation
Negative impact on transmission system	0: None	9: Instigation of instabilities
Negative impact on billing functions	0: None	9: widespread loss of accurate power usage data
Privacy Loss	0: None	9: All stakeholder private data leaked

C. LIKELIHOOD ASSESSMENT CRITERIA

Keeping consistency with the impact assessment criteria, the likelihood assessment criteria are adapted and scaled NESCOR criteria to VPPs. Table II summarizes them.

TABLE II. Likelihood Assessment Criteria

Criterion	Scoring	
	Minimum Score	Maximum Score
Skill required	0: Deep domain knowledge and ability to create custom attacking tools	9: Basic domain understanding and computer skills
Accessibility	0: Air-gapped, solid access controls	9: Internet facing, no access controls
Attack Vector	0: Theoretical	9: Multiple widely exploited techniques
CVE	0: None known	9: Known, commonly used CVEs in unsupported and/or legacy assets

By combining the impact and likelihood criteria and by cross-examination with the security profile for relevance, a high-level risk representation of threats was performed. The next section describes our preliminary findings.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

IV. CRITICAL THREATS AGAINST VPPS

In this section, our findings of VPP threats will be presented, after examining the threat landscape. The context of each threat is first examined, a risk representation is then presented, alongside with possible attack vectors that can manifest the threat and, finally an example scenario is described.

A. OBSTRUCTION OF INTERACTIONS BETWEEN THE VPP AND THE ENERGY MARKET

The physical electricity grid consists of various parts with distinct roles. Generation is where electrical energy is transformed from other energy sources; transmission is the part of the system that transfers the energy from one point to another, distribution is the part of the system responsible for distributing the energy to the consumers and, finally, consumption is the part where electrical energy is converted to other forms of energy. Depending on their generation capacity, DER is usually physically connected to the distribution part of the grid.

The energy market then consists of the producers, who generate electrical energy and sell it to the consumers, the Transmission System Operators (TSOs), who are responsible for the grid's stable and reliable transfer of energy over long distances, the Distribution System Operators (DSOs), who are paid to deliver the energy to the consumers, and the regulating authorities, who monitor and regulate the market.

Even though a VPP can participate in the retail market, there is little adversarial activity to jeopardize it, and we deem it out of the scope of our study. We focus on the VPPs participation in the wholesale market, which consists of the following parts:

- The forward market, where contracts can be weeks or years in the future,
- The day-ahead market,
- The intraday market, or spot market,
- The ancillary services market, which offers demand response and compensation services.

Considering the operation of a VPP within the energy market, their role is crucial for coordinating DER generation and dispatch. As aggregators of multiple DER, they participate in the day-ahead, intraday, and ancillary services markets. Since the cost of production is minimal to zero, due to the renewable nature of most of the aggregated DER, and in combination with the prioritization of renewable generation in scheduling, the ability of the VPP to securely interact with the energy exchange, as well as direct market sellers, by nature of bilateral contracts, is mission critical for the economic stability and profitability of the VPP.

From the entirety of the grid point of view, VPPs can and do exceed 1000MW of generation capacity. This makes them comparable to thermoelectric and nuclear power plants. Unlike those power plants, the economic strategies of VPPs are based on accurate weather forecasting and optimal dispatch scheduling. Interruption of these information flows can deprive the system of gigawatts of power, and since DER interact with load curve calculations by "shaving" the load curve, manifest unexpected load peaks that can congest the transmission system or create system instabilities.

There are two possible ways that an adversary can threaten this VPP mission objective. Firstly, interruption of communication is possible in cases where custom software is being used to facilitate this interaction. This interface is usually provided to the VPP operator as Software-as-a-Service, which would then classify these software solutions as part of the supply chain for the VPP. Standard Denial-of-Service techniques, such as flooding and Distributed Denial of Service (DDoS) against the software provider or the VPP can induce delays and interruptions that can impact the ability of the VPP to offer ancillary services, as well as interacting with intraday markets. Secondly, data tampering vectors can prove just as devastating, as the VPP operator is deprived of their ability to make correct decisions. These can take the form of falsified load forecasts, system state estimation, grid measurements, market pricing forecasts etc.

Table III and Table IV summarize the impact and likelihood assessment of the threat as follows:

TABLE III. Impact Assessment of Market Interruption Threat

Criterion	Assessment	
	Score	Comments
System scale	9	A Shutdown of the market interface affects the operation of the entirety of the VPP, so every DER is affected.
Safety	0	No expected physical impacts that create hazardous conditions are expected.
Financial Impact on VPP	1	Assuming that the VPP partakes in the day ahead, ancillary market and spot market, the attack can disrupt the operation of the VPP for up to a few days. This will represent less than 1% of yearly revenue.
Negative impact on generation capacity	0	Generation functions are not impeded without presence of further faults.
Negative impact on the energy market	9	This is the target of the threat; total market disconnection is expected.
Negative impact on transmission system	2	Some transient effects if DER are automatically disconnected.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	0	Vectors examined do not include data exfiltration techniques.
Total Score	2,62	

TABLE IV. Likelihood Assessment of Market Intruption Threat

Criterion	Assessment	
	Score	Comments
Skill required	9	Attacks against web-facing IT infrastructure are very common and tools for performing the attack are widespread (even legitimate offensive security tools).
Accessibility	9	Internet facing interface.
Attack Vector	9	Multiple, widely exploited and well documented techniques.
CVE	9	We expect them to be present due to legacy equipment.
Total Score	9	

CVEs are expected to be present and exploitable since operational data from the DER is essential to the operation of the VPP and patching of CVEs, if possible, on legacy equipment, requires intensive preparation and can only happen during scheduled maintenance windows.

While there are no recorded attacks against this function, incidents like the partial decoupling of the market in June 2019 [19] are indicative of such possible impacts. A corrupted file was the root cause of a series of events that led to partial decoupling. Similar effects can be caused through adversarial means.

B. FALSE DATA INJECTION IN THE SUPERVISORY AND CONTROL LAYER

False Data Injection attacks have been thoroughly studied in the past years. From GOOSE poisoning attacks [20], Load Redistribution Attacks [21]the focus in the LAA literature has been only on static load altering attacks, where the attack is mainly concerned in changing the volume of the load. In contrast, in this paper, we address dynamic load altering attacks (DLAAs, attacks against inverters [22] and in-state estimation [23]. The intention of these attacks is to insert realistic data into a communications channel with the intention of forcing cyber-physical elements to diverge from their intended operation. They can take the form of either spoofing data, or tampering, by capturing and altering legitimate traffic.

Information about the operational status of the DER is generated by a third-party software specific to the installed manufacturer or maintainer. Communication protocols are assumed to be standard industry-specific, IEC 61850 MMS/GOOSE, DNP3, Modbus at substations. Communication between the third-party software and the platform is assumed to not be fully air-gapped due to the topological distribution of DER and the lack of proprietary communication infrastructure. The load's state and general substation characteristics, like bus voltages and angles, are communicated to VPP operators by DSOs. These protocols have known weaknesses that are difficult to mitigate, partly because their design did not include cyber-security, or their operational reliability requirements hinder them from performing security functions due to constraints of the operational environment.

VPPs have unique supervisory and control environments that differentiate themselves from traditional SCADA infrastructures. They are, however, required to interoperate with DSO SCADA systems. As a result, when considering threats against this function, they may be case-specific to the implementation of each VPP. It is implied in the implementation of the aforementioned protocols that they are operating in trusted network segments.

Attack vectors that can enable the threat, among others, can be: supply chain compromise, remote service exploit, unauthorized command message injection, masquerading attacks, and blind false traffic injection [24].

Table V and VI summarize our evaluation impact and the likelihood of the threat.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

TABLE V. Impact Assessment of FDI attacks

Criterion	Assessment	
	Score	Comments
System scale	9	A compromise of the Supervisory monitoring and Control Platform has the potential to affect all DER connected to the VPP
Safety	7	Unsafe conditions are possible, due to stress to transformers and faulty breaker operation
Financial Impact on VPP	1	Assuming that the VPP partakes in the day ahead, ancillary market and spot market, the attack can disrupt the operation of the VPP for up to a few days. This will represent less than 1% of yearly revenue.
Negative impact on generation capacity	9	Disturbance expected to affect more than10% of generation for more than 8 hours´.
Negative impact on the energy market	5	The VPP can participate in the market, but DER optimization can be severely impeded.
Negative impact on transmission system	9	Instigation of instabilities is possible in unplanned DER connection and disconnection, as well as inability to provide ancillary services.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	0	Vectors examined do not include data exfiltration techniques.
Total Score	5	

TABLE VI. Likelihood Assessment of FDI attacks

Criterion	Assessment	
	Score	Comments
Skill required	9	Attacks against web-facing IT infrastructure are very common and tools for performing the attack are widespread (even legitimate offensive security tools).
Accessibility	9	Internet facing interface.
Attack Vector	9	Multiple, widely exploited and well documented techniques.
CVE	9	We expect them to be present due to legacy equipment.
Total Score	9	

An example of this scenario is an adversary changing the maximum power setpoint of inverters in PV installations. VPPs naturally change this setpoint as a response to market signals. A malicious alteration by means of an unauthorized command message injection can lead to shut down of the inverter [13]. By extension, such a command sent to multiple inverters at the same time can shut down multiple DER at once.

C. DENIAL OF SERVICE OF CONTROLLED ELEMENTS

Electrically, DER are connected to the distribution network, either in the Medium or Low Voltage substations. For DSOs SCADA needs, DER provide communication links to the respective substation to provide electrical measurements, like voltages, current values, power output, power factor etc., as well as establish communications with the VPP operator. Interoperability and backwards compatibility of equipment is paramount to establish a functioning and reliable communication link. They can be wired, through twisted pair cables, optic fiber, power cables, or wireless, through ZigBee, WLAN, GSM, or Z-wave. Topologically, they are connected on a star or mesh grids with the VPP operator. Communication protocols that are used to implement supervisory and control functions are:

- IEC 60870-104 and their derivatives, like DNP3
- Modbus
- IEC 61850, GOOSE and SV for substation automation, MMS, or XML for DER-VPP communication.

The design of IEC 61850, being object oriented and providing interoperability and backwards compatibility options, is gaining traction on becoming the de facto protocol of choice for Smart Grid implementations, especially in Europe. IEC 62351 is the relevant security standard for securing IEC 60870-104 and derivatives, as well as IEC 61850 protocols. However, due to the performance requirements of IEC 61850, modern encryption implementations are sometimes not possible. Even with the augmentations of IEC 62351, these protocols are not fully protected, e.g., the trust architecture is based on embedded X.509 certificates on equipment, which cannot be revoked [25], RSA 1024 used for digital signatures deemed unsafe by NIST, HMAC schemes requiring pre-shared keys. In particular, the fact that certificates are hard embedded in equipment makes physical security of the infrastructure crucial, which is then obstructed by the fact that DER can be located in hard to reach and monitor locations. A motivated adversary could physically access equipment and extract the keys directly from the circuitry of the equipment.

Apart from these inherent weaknesses, these

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

protocols are often mapped to the TCP/IP protocol below the transport layer of OSI, which implies they are susceptible to common flooding and distributed DoS attack vectors. DoS, however, can manifest through FDI vectors as well, when the attack locks the equipment in reboot loops, activates test operation (which is a misconfiguration option), or locks them in update mode. Subtler and more specific vectors can include timing violations, such as withholding packets over the TAL (Time Allowed to Live) threshold or changing the time parameter of the packets, which effectively makes the equipment inoperable.

Performing a dependency analysis on the threat scenario, we also identified that Byzantine failure state induction is also possible. Due to the inherent statistical discrepancies of Smart Grid data, the possibility of Byzantine sensors, IEDs and data [26] is possible. Byzantine state in the VPP setting can take three forms:

1. Equipment compromised and intentionally misconfigured,
2. Failed equipment, where status is being denied or disrupted from being communicated, e.g., alarm suppression
3. Hidden failure that has been intentionally or unintentionally induced.

In a trusted environment, as described above, it is particularly challenging to identify the compromised equipment and reestablish normal operation and the root of trust. When protective equipment is involved or directly targeted, like the TRISIS malware [6], hazardous conditions can be present, including the danger of electrocution. Apart from human safety hazards, Safety Instrumentation Systems (SIS) in a Byzantine state may fail in the presence of non-adversarial faults, causing damage to the infrastructure or interrupt operation without any faults present, causing financial losses.

Table VII and VIII summarize our ratings for impact and likelihood assessment.

TABLE VII. Impact Assessment of DoS attacks on controlled elements

Criterion	Assessment	
	Score	Comments
System scale	0	This is a targeted attack against specific DER.
Safety	9	Byzantine failure state of protective equipment can cause electrocution.
Financial Impact on VPP	3	Physical damage can exceed 1% of yearly revenue.
Negative impact on generation capacity	1	Expected to impact less than 3% of generation capacity.
Negative impact on the energy market	0	The VPP can participate in the market, DER optimization can be slightly impacted.
Negative impact on transmission system	9	Instigation of instabilities is possible in unplanned DER connection and disconnection, as well as inability to provide ancillary services.
Negative impact on billing functions	0	Power usage data are not expected to be affected.
Privacy Loss	2	Data can be exfiltrated, limited to target DER.
Total Score	3	

TABLE VIII. Likelihood Assessment of DoS attacks on controlled elements

Criterion	Assessment	
	Score	Comments
Skill required	2	Substantial domain knowledge needed, ability to adapt existing offensive tools.
Accessibility	9	Internet facing interfaces possible.
Attack Vector	3	Exploited by high profile threat groups.
CVE	9	We expect them to be present in legacy equipment.
Total Score	5,75	

Communication delay between elements of the VPP will further be examined. Time delays on electrical measurements can adversely impact system stability [27]the paper presents a power system model based on delay differential algebraic equations (DDAE, as well as induce oscillations in the power output of the VPP [28]. These can have subsequent impacts on other subsystems of the VPP, like the pitch angle control of wind generators.

V. CONCLUSIONS

Threat assessment in Smart Grid environments is nontrivial but a critical part of risk assessment. In the case of VPPs, this is further exacerbated by the distributed, non-standardized patchwork of different technologies, operating environments, and communication implementations. Diverse ownership of DER, interoperability requirements, Quality of

Service requirements increase the complexity of the system and allow for security gaps to be overlooked.

In order to overcome these problems, we constructed a generalized security profile for VPPs, elected and scaled evaluation criteria, and examined the threat landscape as it translates to VPP environments.

Taking into consideration the inherent gaps in security for Smart Grid communications and implementation, our preliminary findings suggest that FDI attacks remain a prominent threat for VPPs and can affect them in all their operational functions. The trust architecture of VPPs relies greatly on third-party trust relationships between the VPP, DER and third-party implementation solutions. VPP operators are left with no choice but to replace compromised equipment, as it cannot be reinstated in a trustworthy state. DoS attacks are also prominent, as a successful attack may threaten grid stability as well as impact the generation capacity of VPPs. Finally, compromising the interaction between VPP and energy markets can endanger market functions as a whole.

VI. FUTURE WORK

The next stage of our work will focus on expanding on scenarios revolving around the identified threats, by utilizing attack-fault trees to include physical errors that can be induced by the execution of each scenario. An attempt to create correlations between these reactions and anomalous behavior of IT elements will be made and Indicators of Compromise that take into consideration physical system responses and measurements will be constructed.

ACKNOWLEDGMENTS

This publication is partly a result of SecDER project, funded by the German Federal Ministry for Economic Affairs and Energy (BMWi).

REFERENCES

[1] G. Plancke, K. De Vos, R. Belmans, and A. Delnooz, “Virtual power plants: Definition, applications and barriers to the implementation in the distribution system,” Int. Conf. Eur. Energy Mark. EEM, vol. 2015-Augus, 2015, doi: 10.1109/EEM.2015.7216693.

[2] CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, “CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Information Security,” no. November, pp. 1–107, 2012, [Online]. Available: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

[3] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, “Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties,” Energies, vol. 10, no. 1, pp. 1–21, 2017, doi: 10.3390/en10010087.

[4] X. Gao, X. Li, and X. Yang, “Robustness assessment of the cyber-physical system against cascading failure in a virtual power plant based on complex network theory,” Int. Trans. Electr. Energy Syst., no. June, pp. 1–27, 2021, doi: 10.1002/2050-7038.13039.

[5] Robert M. Lee, Michael J. Assante, and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” Ics.Sans.Org, pp. 2–11, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[6] Dragos Inc., “TRISIS Malware,” pp. 1–19, 2017, [Online]. Available: https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=40B2ED59-D34E-47C3-B9E2-1E8D030C5748.

[7] O. T. Soyoye and K. C. Stefferud, “Cybersecurity Risk Assessment for California’s Smart Inverter Functions,” 2019 IEEE CyberPELS, CyberPELS 2019, 2019, doi: 10.1109/CyberPELS.2019.8925257.

[8] M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger, and A. Somani, “A Review of Cybersecurity Risk and Consequences for Critical Infrastructure,” Proc. - 2019 Resil. Week, RWS 2019, pp. 7–13, 2019, doi: 10.1109/RWS47064.2019.8971975.

[9] L. Marinos, “European Union Agency for Network and Information Security Smart Grid Threat Landscape and Good Practice Guide Smart Grid Threat Landscape and Good Practice Guide About ENISA Smart Grid Threat Landscape and Good Practice Guide,” no. December, 2013.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

[10] NESCOR, “Electric Sector Failure Scenarios and Impact Analyses – Version 3.0,” no. December, 2015, [Online]. Available: http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf.

[11] E. P. R. I. (EPRI), “Analysis of Selected Electric Sector High Risk Failure Scenarios National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 First Version,” no. September, 2013.

[12] W. G. Temple, Y. Li, B. A. N. Tran, Y. Liu, and B. Chen, “Railway system failure scenario analysis,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10242 LNCS, pp. 213–225, 2017, doi: 10.1007/978-3-319-71368-7_18.

[13] B. J. Kang et al., “Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,” IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, vol. 2015-Octob, 2015, doi: 10.1109/ETFA.2015.7301457.

[14] S. Jauhar et al., “Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios,” Proc. - 2015 IEEE 21st Pacific Rim Int. Symp. Dependable Comput. PRDC 2015, pp. 319–324, 2016, doi: 10.1109/PRDC.2015.37.

[15] Cyber Trust, “D2 . 1 Threat landscape : trends and methods,” no. 2018, p. 250, 2020.

[16] J. Johnson, J. Flicker, A. Castillo, and C. Hansen, “Design and Implementation of a Secure Virtual Power Plant,” no. September, pp. 243–287, 2017, doi: 10.13140/RG.2.2.36603.62244.

[17] S. M. S. Hussain, T. S. Ustun, and A. Kalam, “A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges,” IEEE Trans. Ind. Informatics, vol. 16, no. 9, pp. 5643–5654, 2020, doi: 10.1109/TII.2019.2956734.

[18] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, “Cybersecurity framework smart grid profile,” p. 142, 2019, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf.

[19] NEMO Commitee, “SDAC report on the ‘partial decoupling’ incident of June 7th 2019,” 2019.

[20] N. Kush, E. Ahmed, M. Branagan, and E. Foo, “Poisoned GOOSE: Exploiting the GOOSE protocol,” Conf. Res. Pract. Inf. Technol. Ser., vol. 149, pp. 17–22, 2014.

[21] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, “Dynamic load altering attacks in smart grid,” 2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2015, pp. 1–5, 2015, doi: 10.1109/ISGT.2015.7131791.

[22] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, “Investigation of False Data Injection Attacks on Smart Inverter Settings,” 2020 IEEE CyberPELS, CyberPELS 2020, no. January 2021, 2020, doi: 10.1109/CyberPELS49534.2020.9311541.

[23] R. Lin et al., “False Data Injection Attacks against State Estimation in AC-DC Hybrid Power System,” Chinese Control Conf. CCC, vol. 2020-July, pp. 4302–4306, 2020, doi: 10.23919/CCC50068.2020.9189440.

[24] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks: Characterizations and Countermeasures,” IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1244–1253, 2013, doi: 10.1109/TSG.2013.2245155.

[25] J. G. Wright and S. D. Wolthusen, “Limitations of IEC62351-3’s public key management,” Proc. - Int. Conf. Netw. Protoc. ICNP, vol. 2016-Decem, no. HotPNS, pp. 1–6, 2016, doi: 10.1109/ICNP.2016.7785322.

[26] A. Vempaty, L. Tong, and P. K. Varshney, “Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks,” IEEE Signal Process. Mag., vol. 30, no. 5, pp. 65–75, 2013, doi: 10.1109/MSP.2013.2262116.

[27] F. Milano and M. Anghel, “Impact of time delays on power system stability,” IEEE Trans. Circuits Syst. I Regul. Pap., vol. 59, no. 4, pp. 889–900, 2012, doi: 10.1109/TCSI.2011.2169744.

[28] M. Elkhatib, J. Johnson, and D. Schoenwald, “Virtual Power Plant Feedback Control Design for Fast and Reliable Energy Market and Contingency Reserve Dispatch,” pp. 2969–2974, 2018, doi: 10.1109/pvsc.2017.8366393.

AUTHORS

George Gkoktsis

George Gkoktsis received his Diploma on Electrical and Computers Engineering with specialization field Electrical Energy from Aristotle University of Thessaloniki, Greece in 2015 and his MSc on Information Security from University of London in 2020.
He is currently working as a researcher at Fraunhofer SIT in Germany, in the department of Cyber-Physical Systems Security and affiliated with the National Research for Applied Cybersecurity ATHENE. His research focuses on Electrical Energy System's cybersecurity, Cyber-resiliency for the energy sector and threat modeling for Critical Infrastructures.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762928

G. Gkoktsis,
"Assessing the Cyber Threat Landscape for Virtual Power Plants",
Latin-American Journal of Computing (LAJC), vol. 9 no. 2, 2022.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol IX, Issue 2, July 2022

Memory Forensics: comparing the correctness of memory captures from locked Windows 10 machines using different boot capture vectors

ARTICLE HISTORY

Received 13 March 2022
Accepted 02 May 2022

Jack Dyson
Department. of Computing
Sheffield Hallam University
Sheffield, United Kindom
Jack.E.Dyson@student.shu.ac.uk

Shahrzad Zargari
Department. of Computing
Sheffield Hallam University
Sheffield, United Kindom
S.Zargari@shu.ac.uk

Memory Forensics: comparing the correctness of memory captures from locked Windows 10 machines using different boot capture vectors

Jack Dyson
Department. of Computing
Sheffield Hallam University
Sheffield, United Kindom
Jack.E.Dyson@student.shu.ac.uk

Shahrzad Zargari
Department. of Computing
Sheffield Hallam University
Sheffield, United Kindom
S.Zargari@shu.ac.uk

***Abstract*—**Memory forensics is rapidly becoming a critical part of all digital forensic investigations. The value of information stored within a computer memory is immense; failing to capture it could result in a substantial loss of evidence. However, it is becoming increasingly more common to find situations where standard memory acquisition tools do not work. The paper addresses how an investigator can capture the memory of a locked computer when authentication is not present. The proposed solution is to use a bootable memory acquisition tool, in this case, Passware Bootable Memory Imager. To enhance the findings, three different reboot methods will be tested to help identify what would happen if the recommended warm reboot is not possible. Using a warm reboot and a secure reboot, Passware Bootable Memory Imager was able to successfully acquire the memory of the locked machine, with the resulting captures being highly representative of the populated data. However, the memory samples collected after a cold reboot did not retain any populated data. These findings highlight that to capture the memory of a locked machine, the reboot method is highly successful, providing the correct method is followed.

***Keywords*—**Digital Forensics, Memory Forensics, Memory Acquisition, Memory Analysis

I. INTRODUCTION

The field of memory forensics was first seen in the early 2000s [1], where methods were very experimental and not widely adopted. Like with many fields in digital forensics, the proposed methods required constant development to tackle the constantly changing technology. It is only in the last decade that memory forensics techniques have gained traction; with more digital forensic practitioners getting involved.

Memory forensics refers to the analysis of a computer physical memory, and its growing popularity stems from the value of information stored in a computer physical memory [2]. Information that would not be present through traditional forensic processes, like hard disk forensics, can be recovered. This includes plain text passwords, encryption keys, cloud storage documents and much more. Plus, the value of memory forensics is growing rapidly. With the increase of out-of-the-box encryption and the growing size of default memory [3], failing to capture a computer random access memory (RAM) could result in a substantial loss of evidence. This is why the traditional approach of "pulling the plug" on a running computer is now less preferred, as it would erase the computer volatile memory. This will undermine Principle 1 of the Association of Chief Police Officers (ACPO) Guidelines for Digital Evidence [4], to preserve the original state of digital evidence. However, a heightened awareness of security is resulting in more situations where standard memory acquisition approaches do not work [5]. For example, when a computer is locked, or the user does not have administrative privileges.

This led to the project research question: I*s it possible to acquire the memory of a locked Windows 10 machine when login credentials are not known?* To answer the research question, this project aimed to *identify whether bootable memory imagers could successfully capture the memory of a locked Windows 10 machine.* Furthermore, to fully investigate the method required for bootable memory acquisitions, an additional aim to *identify how different boot vectors affect the correctness of a memory sample* was explored.

The rest of this report will be laid out in four more sections. Section 2 will discuss a thorough literature review of the existing papers available on memory acquisition tools. Section 3 will

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

explain the methodology that was adopted to answer the research question. Section 4 will explore the results found from the experiment and how they impact the field of memory forensics. Finally, Section 5 will conclude the findings proposed in this report.

II. LITERATURE REVIEW

With memory forensics gaining tracking, there is an increasing number of research papers being released exploring the various challenges that may be faced. The typical approach to capture the memory of a running computer is to use a software-based memory acquisition tool. However, the requirements for these tools to succeed may not always be present. So, it is necessary to explore what alternative methods are available to preserve the memory when the standard tools do not work.

A. SOFTWARE-BASE MEMORY ACQUISITION TOOL COMPARISONS

Software-based memory acquisition tools are small applications, that are run with administrative privileges, which dump the contents of the computer memory into a chosen output file. Lots of research has been conducted into these tools, which has allowed many conclusions to be drawn about which is the best to use. In 2021, Martínez compared the acquisition time of six common open-source memory acquisition tools, as well as their private and shared memory footprint [6]. He concluded that Belkasoft RAM Capturer and DumpIT performed the best overall, with FTK Imager having the largest memory footprint by a very long way, which he noted was a big negative as it could result in lots of data being lost. Martínez ended by stating that "information will be lost if the appropriate tool is not used properly", and that investigators must be considerate of the impact of the tool they are going to use.

Supporting these findings is a similar experiment conducted by Faiz and Prabowo in 2019 [7]. They compared the same tools but looked at additional attributes like the registry impact and loaded Dynamic Link Libraries (DLLs). They found that FTK Imager left ten times more artefacts on the target system than the other tools they tested. Interestingly, part of Faiz and Prabowo's study includes a survey of several companies in America, which showed that FTK Imager was the most popular memory acquisition software of the respondents. This sparks concern that many digital forensic practitioners are not fully aware of the impact of the tools they are using.

However, it is important to note that not all experiments have reflected the same outcomes as those by Martínez and Faiz and Prabowo. In 2020, Mahesan compared the user interface, acquisition time, occupied memory, loaded DLLs, registry changes and portability of FTK Imager, Belkasoft RAM Capturer, DumpIT and Magnet RAM Capturer [8]. Mahesan found that DumpIT was actually the slowest tool tested and it had double the memory footprint of FTK Imager. But, like [6] and [7], he found that Belkasoft RAM Capturer was the best tool in most areas. Overall, he concluded that ranking such tools can be a very difficult and subjective process. These contradicting results emphasise just how unpredictable the performance of software-based memory acquisition tools can be and how the most important thing is that the digital forensic practitioner can explain what impact the tool had on the target system.

B. ALTERNATIVE MEMORY ACQUISITION METHODS

Software-based memory acquisition tools are not the only tools in the market. In 2019, Latzo, Palutke, and Freiling studied many different acquisition methods and produced 'the first survey of forensic memory acquisition that is operating system and hardware architecture independent' [9]. This taxonomy outlined the situations where certain memory acquisition methods should be used to acquire the most memory. These methods ranged from the traditional kernel supported software-based methods to Direct Memory Access (DMA) methods and cold-boot attacks. Kernel level access is required to collect the whole physical memory [6] and without kernel-level access, DMA-based methods and reboot methods are required. However, they expressed how DMA methods can be limited in the size of the memory they can acquire and often need specific settings enabled on the machine to work. They also explained how reboot methods are prone to bit errors as the contents of the memory fades away after a reset. In conclusion of their taxonomy, they showed that there are ways to handle not having kernel-level access and software-based tools are not the only acquisition approach available.

C. MEMORY ACQUISITION OF LOCKED MACHINES

A common use case within law enforcement is to find a running computer that is locked or that does not have administrative privileges. The best way to combat this is to use hardware-based or reboot-based acquisition methods; but they are often either still very experimental,

exploit outdated architecture, or are not widely available. One proposed method was to use a tool called Afterlife [7]. This tool exploits how computers maintain their memory after a warm reboot of the system. Vidas explained how the persistence of memory after a warm reboot was affected by many external factors such as the duration of power loss, the type of memory present and the quality of the components in use. For his experiment, Vidas compiled his own tools to target the Linux operating system. He first populated the memory with a known data set using memfil, then rebooted the machine and captured the memory with Afterlife. Finally, he used memcompare to compare the acquired memory against the known data set memfil had created. His experiment found varying results across different manufacturers and models, which led him to conclude that Afterlife should only be used as a last resort. This implies that more work is required to finesse warm reboot-based acquisition methods. However, it does show that data remains after a warm reboot.

A more modern approach to bypassing the lack of administrative privileges is DCIleach, a hardware-based attack that leverages the Intel Direct Connect interface (DCI) for memory acquisition [6]. This method enables the investigator to directly access the memory, thus bypassing the operating system and any resulting protection. The authors evaluated DCIleach by comparing the difference between a memory capture from a known good software-based memory acquisition tool against a memory capture from DCIleach. Their findings showed that many pages differed, but not many bytes differed, especially in proportion to the size of the memory in use. Though the results sounded promising, in practice, DCIleach would not be feasible as Latzo, Schulze, & Freiling expressed their frustration that it regularly crashed and took an extremely long time to acquire the memory. Additionally, the exploit is only possible if DCI is enabled for the Central Processing Unit (CPU) before the tool is used.

D. MEMORY ACQUISITION QUALITY EVALUATION

The literature reviewed so far has provided and has shown numerous bespoke methods to check the success of memory acquisition methods. Yet, there is still no singular accepted method to judge the quality of a created memory capture or the success of a memory acquisition tool. However, in 2012, Vömel and Freiling attempted to formalise the criteria that determine the forensic soundness of a memory acquisition tool [12]. They proposed that memory captures should be correct, atomic, and integral. Correctness refers to the percentage of memory that has been acquired correctly, atomicity refers to the image not being affected by signs of concurrent activity and integrity refers to how similar the memory capture is to the actual memory at the time the acquisition began. At the time the article was written, Vömel and Freiling did not provide any reproducible methods by which somebody could test their memory sample for correctness, atomicity, and integrity. Instead, they theorised how different acquisition methods would present the three criteria.

Following the formalisation of the memory acquisition criteria, a black box methodology to evaluate the atomicity and integrity of memory acquisition was defined by Gruhn and Freiling in 2016 [13]. Their techniques were said to be 'generalizable, to examine further memory acquisition procedures on other operating systems and platforms'. Similar to Vidas' experiment, Gruhn and Freiling used a custom application, called RAMMANGL.exe, to allocate memory regions with a specific value, which could then be statistically analysed to estimate a comparable atomicity and integrity value. They concluded that reboot attack vectors all present near-perfect point in time integrity and perfect atomicity, due to system activity being halted during the boot.

One other way to check that a memory acquisition tool succeeded is to manually analyse the resultant memory sample to check what artefacts were collected. The forensic memory analysis process has been covered in lots of detail [8]. The Art of Memory Forensics book [9] provides a comprehensive breakdown of the entire field of memory forensics before diving into the analysis of memory captures from Windows, Linux and MAC operating systems, using the Volatility Framework. They specifically explain how Volatility parses the memory captures for known data structures so that the results are informed and contextualised. Even with its age, this book is still a major point of reference for everyone with an interest in memory forensics.

E. PROBLEM DOMAIN

Memory forensics is still a very developing field of digital forensics. Year on year, more research is being done to attempt to bring the forensic soundness of traditional forensic procedures into the unpredictable discipline of memory forensics. Software-based memory acquisition for all major operating systems has been covered in-depth, there are many resources

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

available for practitioners to use to aid their choice of tools. In most cases, these tools will suffice, but it is clear that the frequency of finding locked machines at crime scenes is increasing. This, paired with the lack of available methods to acquire the physical memory of a device when they are locked, illustrates a clear gap in the field of memory forensics that needs addressing. Currently, the proposed methods of acquiring memory from locked machines are through using hardware-based tools, which have been shown to have limited success. One tool that supposedly provides a solution to this, is the Passware Bootable Memory Imager. It can 'acquire a memory image after a warm boot or cold boot of the target machine' [10], allowing it to bypass a lack of administrative privileges. It can also handle secure boot, a new feature for Unified Extensible Firmware Interface (UFEI), the successor of traditional Basic Input/Output System (BIOS), which other bootable memory images cannot do.

III. METHODOLOGY

Unfortunately, there is no standardised methodology available to test memory acquisition tools. Therefore, successful methodologies from previous research into the field have been adopted for this research.

Therefore, a bootable memory acquisition tool was used to attempt to capture the memory of a locked Windows 10 virtual machine. Then, based off methods identified in the secondary research, the acquired memory samples were searched for the presence of known embedded artefacts [11], and the results were compared to a known correct benchmark sample [10]. This allowed the correctness of the memory samples to be witnessed and a qualitative evaluation of the memory acquisition tool to be concluded.

A. EXPERIMENT SETUP

To conduct this experiment with as much control as possible, the memory of a Virtual Machine (VM) with a known data set was acquired. A virtual machine was used as it allowed the physical memory to be reverted to a clean state before the acquisition tool was used. This meant that the later memory captures did not contain traces of the previous acquisitions. Also, despite using a virtual machine in this research, the results are still applicable to physical machines and the steps to run acquisition tool do not differ.

The virtual machine was set up with 8GB of RAM and the Windows 10 Pro 21H1 19041 operating system, which is known to be, is supported by the Volatility Framework [16]. The UEFI firmware was used to allow Secure Boot to be enabled and tested as it is not as widely researched [15]. Finally, to help boot the VM into the UEFI boot manager, the 'bios. bootdelay="5000"' setting was added to the VM configuration file [17], to delay the boot for 5 seconds.

In an attempt to make the experiment as realistic as possible, the virtual machine was populated with a wide range of data. A base dataset was populated to provide a foundation of activity on the VM. No embedded artefacts were populated in the base dataset because they would not reside in the memory at the time of acquisition. Instead, the captured memory would contain the live dataset. This dataset was carefully crafted to include the key artefacts listed in Table II, allowing raw string searches for these artefacts to be conducted. After the live dataset was populated in the VM, it was locked, and a snapshot was taken. This meant the VM could be reverted to that exact state after each memory acquisition was conducted.

B. EXPERIMENT TOOLS

Passware Bootable Memory Imager (PBMI) was chosen to capture the memory of the locked Windows 10 virtual machine. This is a new bootable memory imager that has the capability of collecting the memory of a locked machine, even if UEFI is in use. At the time of conducting this research, this is the only identified memory acquisition tool that used the reboot attack vector, which is capable of bypassing authentication. Though there are other tools available, previous research shows they are not successful and there are no papers discussing the use of PBMI.

For the benchmark comparison memory samples, the virtual memory files ('.vmem' and '.vmss') of the virtual machine were copied and analysed in the same way that the acquired memory samples were analysed. These benchmark files present fully correct, integral, and atomic images of the physical memory, so they provide the perfect sample to be compared against.

Multiple tools were used to analyse the captured memory and they were selected based on their functionality and their popularity. To structurally parse the spatial aspect of the memory captures, the Volatility Framework, an open-source memory analysis platform, was used. Next, to attempt to extract drive

TABLE I. SHOWING THE EMBEDDED ARTEFACTS THAT WERE POPULATED INSIDE THE SCENARIO VIRTUAL MACHINE

Embedded Artefacts		
Artefact	**Value**	**Analysis Tool used to Identify Artefacts**
UUID-1	4c2e31ba-4446-4005-86fd-5440cf7ad775	Volatility (chomehistory, cmdline, filescan, handles) Autopsy (String Search)
UUID-2	99acb322-ed55-4ae8-b199-56e3f7eaa3d5	
UUID-3	af6abd8a-4882-47f4-a631-a1a8cc9f5595	
UUID-4	fb5a0717-1569-4f75-babf-792c71b49f0a	
UUID-5	bae0b5cf-6d89-4cc0-98f8-fc306ad9f0c9	
Process-1	Microsoft.Photos.exe	Volatility (pslist, psscan) Autopsy (String Search)
Process-2	Chrome.exe	
Process-3	notepad++.exe	
Process-4	Discord.exe	
Process-5	VeraCrypt.exe	
Password-1	PurplePaper8	Passware Kit Forenisc (Memory Analysis) Autopsy (String Search)
Password-2	OrangeWave7	
Password-3	CyanWheel4	
Password-4	CrimsonLight0	
Password-5	LimeMouse3	
FileName-1	Starfish.jpg	Volatility (filescan, handles) Autopsy (String Search)
FileName-2	GoogleDriveDoc	
FileName-3	APT_FiveEyes.yar	
FileName-4	FiveEyes.yar	
FileName-5	GenericFile.txt	
Executable-1	ChromeSetup.exe	Volatility (cmdline, shimcachemem) Autopsy (String Search)
Executable-2	VSCodeUserSetup-x64-1.62.2	
Executable-3	DiscordSetup.exe	
Executable-4	Testlimit64.exe	
Executable-5	npp.8.1.9.2.Installer.x64.exe	

TABLE II. PASSWARE'S RECOMMENDED METHOD TO CONDUCT EACH REBOOT AND THE EQUIVALENT POWER OPTIONS AVAILABLE IN VMWARE

Reboot Vector	**Passware's Recommendation**	**VMware's Equivalent**
Warm-Boot	Hardware Reboot/Reset button	'Reset' power option
Cold-Boot	Hardware Power Off and Power On	'Power Off' power option
Secure-Boot	Hardware Reboot/Reset button	'Reset' power option

encryption keys and login details, Passware Kit Forensic was used. This is the commercial analysis platform that deploys PBMI, and it now comes with its own memory analysis feature. Also, Autopsy, an open-source forensic analysis platform, was used to conduct a raw string search for the embedded strings. Finally, for benchmark comparison purposes, HxD Hex Editor was used. This is an open-source hex viewer capable of statistically analysing large files to get a percentage of the number of times each character appears. The proposed backup analysis tool was AccessData FTK Imager, a lightweight, free, data preview tool because a comprehensive analysis can be done with just a raw string.

C. MEMORY ACQUISITION PROCESS

Passware Bootable Memory Imager (PBMI) was used to acquire the memory of the VM. It was used five times for each boot vector to account for any anomalous results. Each time, the memory captures were copied off the drive to stop PBMI overwriting the previous captures. To successfully capture the memory with PBMI, Passware recommends that the reboots are done in a specific way [10], Table II shows the equivalent power options provided by VMware.

D. MEMORY ANALYSIS PROCESS

Based on Gruhn and Freiling's work in 2016 [13],

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

the atomicity and integrity of a boot acquisition tool can be assumed, so only the correctness of the samples needed to be compared. Unfortunately, there is no set method how to check the correctness of a memory capture. Traditional forensic methods, like hashing, will not work because it is near impossible to obtain two identical memory dumps [6]. Instead, the contents of the memory should be checked for the presence of known artefacts.

To check for these embedded artefacts, a forensic workstation containing the Volatility Framework, Passware Kit Forensic and Autopsy Digital Forensics were used. The results were quantified and compared against the fully correct benchmark memory sample. Additionally, HxD Hex Editor was used to compare the whole contents of the acquired memory dumps to the contents of their benchmark sample. However, as PBMI must run on a FAT32 filesystem, the acquired memory sample was segmented, with each segment having a custom 64-byte header. Therefore, to try to get Volatility to successfully parse the memory capture, a custom Python script called 'Passware_Amalgamator.py' was created which removes the 64-byte headers and combines each segment into one binary file.

1) Volatility Framework

The Volatility Framework was used to structurally parse the memory samples. It uses an operating system profile to parse the memory capture for the structures defined in a given plugin. Numerous plugins were used for this analysis, including imageinfo, pslist, handles, filescan, consoles, shimcache and chromehistory. To quantitatively record the success of the plugins, the plugin results from acquired samples were compared against the same plugin results from the benchmark memory capture and they were given the following qualitative value of:

- 1 if the plugin worked and the results closely matched the benchmark test.
- 0.5 if the plugin worked but the results did not match the benchmark test.
- 0 if the plugin failed to parse the memory image.

2) Passware Kit Forensic

Passware Kit Forensic was used to identify any passwords in the scenario VM, in particular the manually embedded passwords. To quantitatively record the success of Passware Kit Forensic memory analysis capability, the total number of passwords that were recovered was noted and the following additional qualitative score was given for the identification of the embedded passwords:

- 1 if the embedded password was found.
- 0 if the embedded password was not found.

3) Autopsy Digital Forensics

Autopsy Digital Forensics was used to manually check whether PBMI managed to extract the embedded artefacts in Table I, without the need for it to be parsed by an external tool. To quantitatively record the success of the manual search, the memory samples were opened in Autopsy and a keyword search containing the embedded strings was run. The number of hits for each artefact was recorded.

4) HxD Hex Editor

HxD's statistics analysis feature was used to create a bar chart of the percentage occurrence of each character in the acquired memory samples and the benchmarks. These graphs were visually compared to identify how similar the contents of the memory files were to the benchmarks.

E. METHODOLOGY LIMITATIONS

The proposed methodology is not without limitations. Firstly, the dataset was only created in a short timeframe, which is not reflective of a real-world scenario. But as the main focus of this report is on the volatile data this is not a major issue. What was of more concern, was that to enable Secure Boot, the VM needed to be powered off. This meant that two datasets were required for the experiment, so comparisons were slightly skewed. To control this, the steps taken to create the live dataset for each boot vector were reproduced and documented precisely.

Another limitation was that only one commercial memory acquisition tool was tested. Unfortunately, due to a global chip shortage, the hardware for the other methods which could be tested, like PCIleach, could not be obtained. As a result, the study does not show all of the tools available to an investigator to capture the memory of a locked machine, but it does show to what extent it is possible.

One final limitation was the inconsistent Volatility Framework. Unless the exact profile for the memory sample exists, Volatility may

not be able to parse the appropriate data structures, rendering the tool useless. This is why the VM was carefully set up to be using a profile Volatility supports. Despite this, Volatility was still unable to find the address space of the memory samples created by PBMI, even though it could correctly parse the benchmark samples. Passware was contacted about this issue and attempted to produce a fix. Though they managed to get PBMI to work with Volatility, this experiment had no success.

IV. RESULTS AND DISCUSSION

Passware Bootable Memory Imager successfully captured 8GB of data with all five acquisitions for all reboot vectors. The SHA-1 hash values of these memory samples all differed, highlighting that the captured data was different, but this is expected as a computer memory is always changing. So, even though the acquired snapshot contained the same dataset each time, uncontrollable factors would inevitably lead to minor differences in content, resulting in the different hash values. Despite these differences, it is very encouraging that the tool was able to capture something when the computer was locked. However, to assess the quality of what PBMI was able to capture the correctness of the memory samples would need to be analysed.

A. BENCHMARK ANALYSIS

Yet before these acquired memory samples could be analysed, a known correct benchmark needed to be collected for comparison purposes. The benchmark samples are identical copies of the locked virtual machine physical memory before the reboot took place. This would show a fully correct example of what artefacts could be found in the memory of the VM. A benchmark sample was collected for each of the reboot snapshots so that the comparisons were as accurate as possible.

The structured analysis with the Volatility Framework showed that all the desired plug-ins worked for the three benchmarks. This indicates that the physical memory of the virtual machine before the reboots was very similar, which ensures that accurate comparisons with the memory captures can be drawn. To attempt to find references to the embedded passwords, Passware Kit Forensic was used. Unfortunately, it could not parse any of the embedded passwords in the benchmark samples, but it did identify many other passwords. Though the other passwords held no obvious relevance to the populated dataset, the number of these additional passwords retrieved is an ideal benchmark value for comparison with the acquired memory samples. Finally, Autopsy was used to conduct the raw string keyword search for the key embedded artefacts. These results showed that all of the artefacts, aside from Password-2, Password-3 and Password-5 were found at least once in all of the benchmark samples. This clarified that no references to these missing artefacts would be present in the acquired memory samples, as they were not even present before the reboot.

It is worth noting that there were some minor differences between the content of the warm and cold boot benchmarks to the secure boot benchmark. Two fewer passwords were identified by Passware Kit Forensic, and two fewer artefacts were found by the raw string search, including no reference to Password-5. These differences are expected because the secure boot benchmark was copied from a different virtual machine snapshot. But the presence of these artefacts in the benchmark samples show that the population of the virtual machine was highly successful. Meaning the acquired memory samples can be effectively compared to a known correct image of the virtual machine's physical memory.

B. WARM BOOT ANALYSIS

A warm reboot is the recommended method of acquiring the memory of a locked machine with PBMI. Unfortunately, the structured analysis of the warm boot samples was unsuccessful. As we can see in Fig 1, all of the Volatility plug-ins failed to work, even though they worked on the benchmark sample. The error raised by Volatility states that 'No suitable address space mapping [could be] found', meaning that the structural information required to parse the memory dump was not found in the memory captures. This information was present before the reboot, as the benchmark sample worked correctly, so the fact it could not be found afterwards implies that the acquisition tool was unable to collect this data correctly.

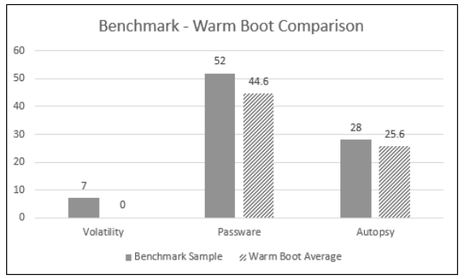


Fig. 1. Showing a comparison of the average scores for the warm boot samples, against the warm boot benchmark sample.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

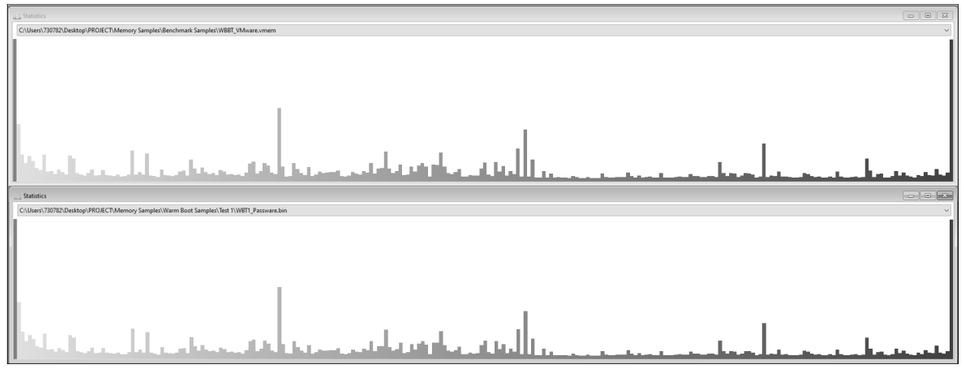


Fig. 2. Showing the percentage occurrence of each character located in the warm boot benchmark (top) and the warm boot Sample 1 (bottom).

As anticipated from the benchmark analysis, none of the embedded passwords were parsed using Passware Kit Forensic, but an average of 44.6 other passwords were found. This value is below the benchmark score, but interestingly, Sample 3 only identified 20 other passwords. Whereas the other four samples found over double that value, suggesting that Sample 3 could be an anomalous result. If this result was removed, it would increase the average score to 50.8, which is much closer to the benchmark and more representative of what would be expected from the warm reboot attack vector. Equally, this does reinforce the volatile nature of memory forensics.

Contrastingly, the results for the raw string search were a lot more consistent across the memory samples. On average, 25.6 artefacts were identified, and every artefact, aside from Password-2 and Password-3, was found at least once. The presence of these artefacts across all of the memory samples emphasises that the warm boot acquisition was successful at capturing the majority of the memory. Thus, supporting the hypothesis that the warm boot does not affect the correctness of the memory samples.

Further supporting the success of the warm boot reboot vector is Fig 2. This depicts how closely the content of the warm boot memory sample matches the content of the warm boot benchmark. They are not identical, and it does not show where the characters were located, but it does emphasise how similar their contents are.

C. COLD BOOT ANALYSIS

A cold reboot is easier to achieve than a warm reboot, as it only requires the power to be turned off and back on using the power button. However, it is hypothesised that this removal of power should wipe the volatile memory before it can be captured, rending PBMI useless. Once again, the structured analysis was ineffective, with no plugins producing any results. The same error was produced as with the warm boot samples, highly likely due to the same issue with the acquisition tool. Unfortunately, this does not help to support the hypothesis as the results do not illustrate what is in the contents of the memory.

On the other hand, with Passware Kit Forensic, we start to see the first evidence supporting the hypothesis. Displayed in Fig 3, no passwords could be parsed across all cold boot memory samples. It was expected that the embedded passwords would not be found. But as no other passwords were found either, it implies that the captured memory does not contain any traces of the populated activity that was present before the cold reboot.

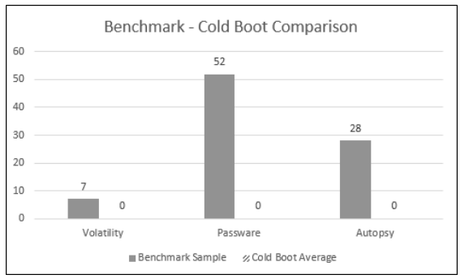


Fig. 3. Showing a comparison of the average scores

for the Cold Boot Samples, against the Cold Boot Benchmark Sample.

Strengthening the Passware Kit Forensic analysis, we can see that the autopsy raw string search found no keyword hits for any of the embedded artefacts. This is critical because it exposes that, even with the most basic form of analysis, no reference to the populated data remains. The data that is present, is likely traces of activity populated after the cold reboot. These results confirm the hypothesis that the cold reboot cleared the volatile memory due to the removal of power.

But what is most illustrative of the impact of the cold reboot is Fig 4. It shows just how different the acquired cold boot memory sample is from the benchmark sample. HxD's statistical analysis of the content of the cold boot memory sample found that 99.88% of the file contained null bytes, in contrast to the benchmark which had just 33.28% null byte coverage. These stark figures clearly support the hypothesis that the cold reboot wiped the memory, thus, drastically affecting the correctness of the acquired memory samples.

D. SECURE BOOT ANALYSIS

A secure boot is a new UEFI boot feature that requires bootable applications to be signed and verified before they can be run. This is raised as a potential pitfall for bootable memory acquisition tools, hence why it has been tested. For PBMI to capture the memory of a locked machine with secure boot enabled, additional steps and an extra reboot were needed. Due to this additional time and the extra reboot, the hypothesis that the correctness of the memory would be slightly affected was drawn. Once more, the Volatility Framework failed to structurally parse any of the memory samples because of the same error. This error occurred for all samples across all boot vectors, leaving the only constant to be the acquisition tool itself.

Logically, Passware Kit Forensic was unable to parse any of the embedded passwords, as they were not even retrieved from the benchmark sample. However, some other passwords were retrieved, resulting in an average of 48 passwords being found. Interestingly, the secure boot maximum value of 50 passwords is lower than the warm boot sample maximum of 52 passwords. However, the secure boot average is higher than the warm boot average, caused by the anomalous warm boot Sample 3. Omitting the anomalous sample would change the implications of the results because it would suggest that the warm boot was able to retain more of the memory than the secure boot. Either way, the secure boot results show that some of the populated data could be retrieved from all of the memory samples.

From the raw string search, all of the embedded artefacts that were found in the secure boot benchmark analysis were retrieved across all of the secure boot samples. These results demonstrate that after a secure reboot the majority of the virtual machine physical memory will remain. In turn, this implies that it is possible to acquire the memory of a locked Windows 10 machine with secure boot enabled, with minimal impact on the correctness. Interestingly, the average scores from the secure boot acquisitions, seen in Fig 5, are much closer to the benchmark results than the warm boot acquisitions (Fig 2). This opposes what was expected, as it was thought that the additional steps required for the secure boot acquisitions would have had a greater impact

Fig. 4. Showing the percentage occurrence of each character located in the Cold Boot Benchmark (top) and Cold Boot Sample 1 (bottom).

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

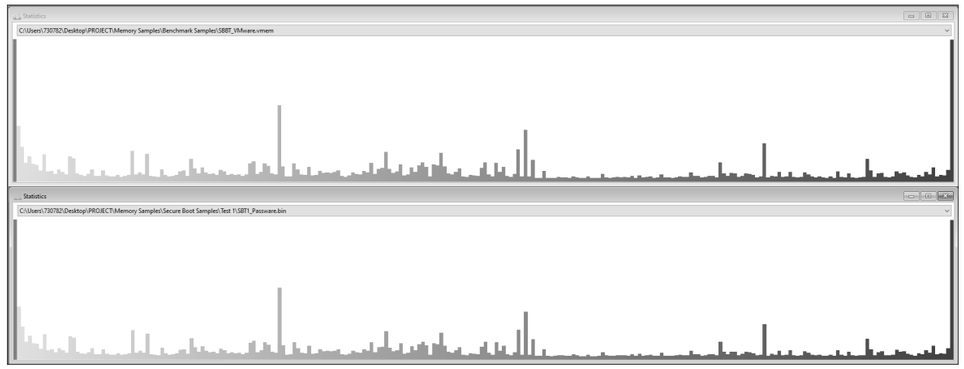


Fig. 6. Showing the percentage occurrence of each character located in the Secure Boot Benchmark (top) and Secure Boot Sample 1 (bottom)

on the correctness of the memory samples. Yet, the results show this is not the case. However, it is worth noting that the benchmark for the secure boot was from a different snapshot, so the populated data may differ, explaining why the secure boot benchmark scores are lower than the warm boot benchmark scores.

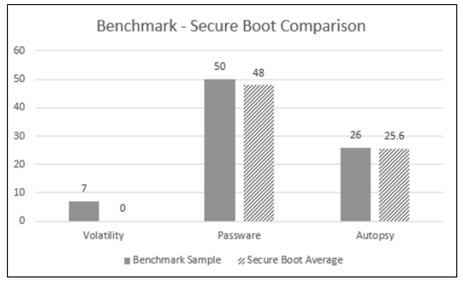


Fig. 5. Showing a comparison of the average scores for the Secure Boot Samples, against the Secure Boot Benchmark Sample.

The final evidence to support how closely the secure boot memory samples matched the benchmark is displayed in Fig 6. This illustrates how the content of the secure boot memory sample is very similar to the contents of the benchmark. Emphasising that the secure boot does allow the physical memory to be retained, and consequently, acquisition with a bootable memory imager has minimal impact on the correctness of the capture. Moreover, it is notable that despite the warm boot and secure boot samples not equally matching their benchmark, the Autopsy average scores are identical. Therefore, it can be inferred that conducting a warm reboot with or without secure boot enabled will result in a very similar memory sample.

E. EXPERIMENT HIGHLIGHTS

To conclude the findings, a wealth of information has been collected from the experiment, which has allowed many insightful deductions to be drawn. Firstly, the importance of memory forensics is exemplified by the wealth of artefacts found in the memory samples of the scenario virtual machine. The plain text Windows 10 user account password was found, alongside numerous other passwords. Plus, there were references to encrypted documents and their contents, which were stored both locally and on a cloud service. This is all vital information that may not be present through standard hard disk analysis techniques.

Next, the experiment showed that even though the virtual machine was locked, it was still possible to capture its memory using a bootable memory imager. Furthermore, the acquired memory was highly representative of the populated data. However, Passware Bootable Memory Imager did struggle to produce memory samples that could be analysed with the Volatility Framework. This is not essential, but it does mean the only way to parse the memory samples would be through more time-consuming, manual analysis.

Finally, the experiment showed that the different boot vectors did have an impact on the correctness of the captured memory. The warm reboot and the secure reboot both acquired most of the memory, but the cold reboot did not retain any of the populated memory. This indicates that it is critical for an investigator to reboot the computer in the correct way, to ensure that the memory is retained. However, it does not matter whether secure boot is enabled on the computer as PBMI can effectively handle this.

Stepping back from this experiment and addressing the wider field of memory forensics, a more extensive study into memory retention after a warm reboot would significantly support the results from this experiment. In 2010, Vidas stated that the amount of time the power is lost for affected the persistence of the memory [11]. Therefore, bootable memory acquisitions should only be used as a last resort. However, this study has shown that bootable memory acquisitions are now much more feasible. So, a more thorough investigation into the factors that impact memory retention after a reboot would be useful. Finally, this research reinforced how key passwords are stored in plaintext within a computer memory. However, these passwords were only found because they were known beforehand. So, exploring whether these passwords could be retrieved, without being known, could significantly aid digital forensic investigations. This could be achieved by identifying whether these passwords are located in the same place within the memory, or whether they are located near constant values that could be searched for instead.

V. CONCLUSIONS

In conclusion, this study has highlighted the importance of memory forensics, and how its value in digital forensic investigations is increasing. The reviewed literature explored the current methods of acquiring memory. However, it exposed an absence of academic research into acquiring memory when certain obstacles, such as a lack of privilege or authentication, are encountered. It was discovered that there were some methods that could tackle these issues: in particular, a reboot attack or a hardware-based attack. After refining the research to those methods, a new reboot-attack tool called Passware Bootable Memory Imager (PBMI) was identified.

As a result, a methodology to test the capabilities of PBMI was developed based on previous research. Using VMware, a virtual machine was populated with a known dataset before it was locked. The memory files of the VM were copied to act as a benchmark of a known correct memory sample, and then PBMI was used to capture the memory. Three different reboot methods were used with PBMI: a warm reboot, a cold reboot, and a secure reboot. Testing these different reboots helped to identify what would happen if the recommended warm reboot was not possible. To assess the correctness of the memory samples, three memory analysis tools were used to quantitatively score each sample on the number of embedded artefacts that were found. Plus, HxD was used to compare the contents of the memory samples.

Based on these quantitative scores, the experiment showed that, with a warm reboot and a secure reboot, PBMI was able to successfully capture the majority of the virtual machine memory. However, the memory samples acquired using the cold reboot were not correct. HxD's statistical analysis of the cold boot sample found that 99.88% of the memory file contained null bytes, whereas the benchmark file only contained 33.28% null bytes. What is more, none of the memory samples acquired through PBMI could be structurally analysed with Volatility, which is a major drawback for memory analysis.

Despite the success of the experiment, there were some limitations to the methodology. Specifically, at the time of writing, PBMI was the only available acquisition tool capable of capturing the memory of a locked machine, and it required the purchase of Passware Kit Forensic for it to be used. This is not desirable considering many other memory acquisition tools are free to use. What is more, no hardware-based tools or open-source tools were available for testing, so the study lacks some breadth. However, the study does provide a proof-of-concept that acquisition of a locked machine is possible, and it has highlighted the importance of avoiding a cold reboot.

Overall, these results have answered the research question. It is possible to acquire the memory of a locked Windows 10 machine, without knowing the login password. Also, the results show that different boot vectors do impact the correctness of the memory capture. Therefore, to retain the information stored in the memory, it is important that a cold reboot is not used. From this study, the reboot attack method to capture the memory of a locked machine has been proven to be highly successful, when the correct method is followed.

A. FURTHER RESEARCH AREAS

Although many areas were addressed in this study, certain questions remain. Firstly, it is a major downfall that structured analysis of the acquired memory samples was not possible. Though manual analysis could be done, automating this process with a memory analysis tool, such as the Volatility Framework, is of utmost importance to investigators. Therefore, it would be key to address why acquisitions with PBMI created memory samples that Volatility could not parse.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

REFERENCES

[1] A. Case and G. Richard III, "Memory forensics: The path forward," Digital Investigation, vol. 20, pp. 23-33, 2017.

[2] A. Chetry and U. Sharma, "Memory Forensics Analysis for Investigation of Online Crime - A Review," in 6th International Conference on Computing for Sustainable Global Development, Delhi, 2019.

[3] C. Tardi, "Moore's Law," 23 February 2021. [Online]. Available: https://www.investopedia.com/terms/m/mooreslaw.asp#:~:text=Moore's%20Law%20refers%20to%20Gordon,will%20pay%20less%20for%20them..

[4] J. Williams, "ACPO Good Practice Guide for Digital Evidence," Association of Chief Police Officers, London, 2011.

[5] Lucideus, "Windows Volatile Memory Acquisition & Forensics 2018 | Lucideus Forensics," 29 October 2018. [Online]. Available: https://medium.com/@lucideus/windows-volatile-memory-acquisition-forensics-2018-lucideus-forensics-3f297d0e5bfd.

[6] M. Martínez, "Impact of Tools on The Acquisition of RAM Memory," The International Journal of Cyber Forensics and Advanced Threat Investigations, vol. 1, pp. 3-17, 2021.

[7] M. Faiz and W. Prabowo, "Comparison of Acquisition Software for Digital Forensics Purposes," Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, vol. 4, pp. 37-44, 2019.

[8] T. Mahesan, "Comparison of Memory Acquisition Software for Windows," 26 Dec 2020. [Online]. Available: https://thanursan.medium.com/comparison-of-memory-acquisition-software-for-windows-e8c6d981db23.

[9] T. Latzo, R. Palutke and F. Freiling, "A universal taxonomy and survey of forensic memory acquisition techniques," Digital Investigation, vol. 28, pp. 56-69, 2019.

[10] T. Latzo, M. Schulze and F. Freiling, "Leveraging Intel DCI for Memory Forensics," in The Digital Forensic Research Conference, USA, 2021.

[11] T. Vidas, "Volatile Memory Acquisition via Warm Boot Memory Survivability," in 43rd Hawaii International Conference on System Sciences, Hawaii, 2010.

[12] S. Vömel and F. Freiling, "Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition," Digital Investigation, vol. 9, pp. 125-137, 2012.

[13] M. Gruhn and F. Freiling, "Evaluating atomicity, and integrity of correct memory acquisition methods," Digital Investigation, vol. 16, pp. s1-s10, 2016.

[14] M. Ligh, A. Case, J. Levy and A. Walters, The art of memory forensics: detecting malware and threats in Windows, Linux and Mac memory, New York: Wiley, 2014.

[15] Y. Gourenko, "How to use Passware Bootable memory Imager," 19 Oct 2021. [Online]. Available: https://support.passware.com/hc/en-us/articles/1500000308641-How-to-use-Passware-Bootable-Memory-Imager.

[16] A. Case, "Volatility Wiki," 17 April 2020. [Online]. Available: https://github.com/volatilityfoundation/volatility/wiki.

[17] VMware, "Configuring and Managing Virtual Machines," 31 May 2019. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-62F39498-1492-4774-A38D-1EDD3DA3C046.html.

AUTHORS

Jack Dyson

Jack Dyson is studying Cyber Security with Digital Forensics at Sheffield Hallam University who is due to graduate 2022. After graduating, Jack will begin to work as a Digital Forensic Analyst with South Yorkshire Police's Digital Forensics Unit.
Since 2020, Jack has spent the last two years working with the Yorkshire and the Humber Regional Organised Crime Digital Forensics Unit, where he spent his time researching and developing new tools and techniques that can be used by police forces across the region. The bulk of his research was into crime scene digital forensic capabilities which included memory forensics.

Shahrzad Zargari

Shahrzad Zargari has a PhD in Applied Statistics and MSc in Forensic Computing & Security (with Distinction). She has worked in the computer industry for over 15 years and gained a great deal of experience in computer hardware, software, and business management.
Shahrzad is passionate about digital forensics and security, advocating collaboration (i.e. Government, Industry & Academia), sharing information and educating students. Her background in applied statistics and data mining allows her to have a unique approach towards cyber security, including intrusion detection.
Shahrzad is an experienced researcher (CENTRIC), having published book chapters as well as many papers in conferences, journals, and magazines. Additionally, Shahrzad is the associate editor of Information Security Journal: A Global Perspective at Taylor & Francis.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762962

Performance evaluation of Mobile Sensor for Context Awareness User Authentication

ARTICLE HISTORY

Received 13 March 2022
Accepted 02 May 2022

Eniola S Adewumi
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8009528@my.shu.ac.uk

Timibloudi S Enamamu
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
t.enamamu@shu.ac.uk

Aliyu A Dahiru
Department of Computing, Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8040371@my.shu.ac.uk

E. Adewumi, T. Enamamu, A. Dahiru,
"Performance Evaluation of Mobile Sensor for Context Awareness User Authentication",
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.

Performance Evaluation of Mobile Sensor for Context Awareness User Authentication

Eniola S. Adewumi
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8009528@my.shu.ac.uk

Timibloudi S. Enamamu
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
t.enamamu@shu.ac.uk

Aliyu A. Dahiru
Department of Computing,
Collage of Bussines,
Technology and Engineering,
Sheffield Hallam University
Sheffield – United Kingdom
b8040371@my.shu.ac.uk

***Abstract*— With the increase of smart devices and their capacities, their use for different services have also increased. As much as this is an advantage, it has posed additional risks because of the confidential information stored on them. This has increased the need for additional security on the smart devices. Most of the methods used for user authentication pose certain drawbacks that are either easy to circumvent or cumbersome to use. As a result, multi-level means of authentication is needed to improve the security of mobile devices. Sensors are playing a vital role in the mobile ecosystem to enhance different services. These sensors can be leveraged upon as a solution for user authentication. This research analyzed and evaluated different mobile device sensors for continuous and transparent user authentication. The mobile data used includes gyroscope, accelerometer, linear accelerometer, proximity, gravity, and magnetometer sensor data. A feedforward neural network was used for data classification. After extracting features from the different sensors available in the mobile device, the most effective sensor was selected by evaluating performance of the different sensors. The best sensor, the accelerometer was further experimented on. The experiment showed that smartphone accelerometer sensor exhibits sufficient discriminability, stability, and reliability for active and continuous authentication, by achieving a performance of 6.55% for the best overall EER.**

***Keywords*— Mobile Sensor, Authentication, Mobile Device, Accelerometer**

I. INTRODUCTION

The number of Internet of Things (IoT) devices is projected to be 120 billion by the year 2025 [1]. The present-day smartphones have the capacity to support the user's needs. As a result, people rely on the services and information on their mobile device to complete their daily activities such as business or personal activities. Some of these daily activities include meeting schedules, accessing emails, online games, online shopping, accessing news, and sharing of documents.

Most recent mobile devices have increased capacity in terms of storage, and this means increase in the storage of sensitive data on such devices. As more of these data are stored in the device, information leakage becomes a concern to organizations and users of these mobile devices.

Researchers from University of Pennsylvania demonstrated how latent smudges leave smartphones susceptible to hacking. Smudges attack is used to obtain PIN and pattern of a smartphone, simply by increasing or decreasing the contrast of the smartphone [2].

Pattern, PIN, and password also suffer from shoulder surfing attacks; this attack occurs when a malicious user can fully observe or watch the login session [3].

Cameras on mobile devices are getting better with increased pixels, therefore, it will be useful for capturing biometric data for user authentication [4] and can be used for spying. Once a user is identified while using a camera, the pictures can be used to fool the system.

Transparent and continuous biometric authentication system should improve the security of mobile devices, it should provide a convenient protection mechanism for mobile devices [5]. To enhance mobile device security with continuous mechanisms, usability should be considered. Out of various authentication solutions, a promising technique is the utilization of sensory data. Unlike other special biometric techniques for smartphone authentication (such as touch behavior or fingerprints), most sensors do not require any

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

specialized hardware to obtain biometric data [4]. Furthermore, from the analysis of most sensors on mobile devices, sensory data can be in a continuous manner if the mobile device is being used. Hence, sensory data from mobile devices can provide a non-intrusive, active, and continuous authentication solution.

Recently, there has been an increase in literature toward sensors behavior for authentication. Research on entry-point authentication [4] [6] as well as active continuous authentication [7] shows multi-motion sensor (such as accelerometer and gyroscope) investigation and analysis. Most research based their work on motion-sensor users' authentication. Nevertheless, the research work using these sensors for motion-based authentication have not been comprehensively evaluated; these sensors need detailed analysis of accuracy, stability, and usability across various application scenarios. Therefore, this paper focuses on evaluating the performance of mobile sensor behavior for active smartphone authentication. Table 1 below shows publications about mobile phone sensors for user authentication.

TABLE I. CONTRIBUTIONS IN USER AUTHENTICATION USING MOBILE PHONE SENSORS

Name of Author	*Year*	*Type of data used*	*Accuracy*	*Conti-nuous/ non-continuous authentication*
Wei and Ruby [16]	*2017*	*Fingerprint and ear pattern*	*90.23%*	*Non-continuous*
Mohammad et. al. [15]	*2017*	*Proximity Sensor*	*97.38%*	*Non-continuous*
Hernandez-Alvarez et. al [17]	*2021*	*Gyroscope and accelerometer*	*76.85%*	*Continuous*
Alqarni et. al. [20]	*2020*	*Hand movement and waving pattern*	*74.9%*	*Continuous*
Papavasileiou et. al. [24]	*2021*	*Gait (Smart socks and smart shoes)*	*EER of 0.01% and 0.16% , respectively*	*Continuous*

In this article, we evaluated the performance of various mobile phone sensors for active and continuous user authentication, the user's environment was also put into consideration. The experiment evaluated the performance of different sensors across various user activities. These sensors data can be fused to increase the authentication accuracy based on a predefined threshold by using the most suitable data for continuous authentication taking cognizance of the environment. To achieve this, the following research objectives were established:

- To investigate the various mobile sensor data suitability for active authentication.
- Evaluate and analyze the different sensor's data based on different activities.
- A further analysis of the best performing sensor.

II. RELATED WORK

There has been various works on different methodology for securing mobile device. It is necessary to improve on these methods as the traditional method of knowledge-based authentication has memorability issue [8] when a complex password or pin is used. Using biometrics like fingerprint, facial and voice print are common methods for mobile device authentication [9]. This is made easy due to the sensor in them and therefore, don't require any installation on the devices [10]. In [11], the use of spoofing for attacking biometric systems was explained, this is on the increase. Hence, the work proposed a 3D anti spoof touchless ear biometric sensor using a laser biospekled fringe projection profilometry based imaging algorithm. The algorithm uses the combination of biospekle analysis and fringe profilometry technique. The accuracy of the techniques is affected by shadows and hair which are unavoidable [12].

In a similar work, a finger imaging using contactless 3D convolutional neural network (CNN) for user authentication was proposed [13]. The imaging framework use Multiview deep learning for extracting the minutiae feature of the fingerprint. This method is used to overcome the problem of elastic deformations of the friction skin and local regions of fingerprint images. This is caused by sweat, dirt, dryness of the skin or skin diseases, and inconsistent finger pressure while extracting the fingerprint. This method, when used can solve the problem of latent lifting in 2D fingerprint authentication.

A similar method like the last two authors was introduced, using fingerprint, and retina for authentication [14]. Here, an RSA (Rivest-Shamir-Adleman) asymmetric cryptographic algorithm for encrypting the biometric template to improve security for authentication was proposed. To reduce error in the process and make it more flexible, any of the two

biometric can be used, and can be fused using it to encrypt the template gotten from the biometric features. They also mentioned that the fusion of the three biometric features would reduce the error, provide flexibility, and build resistance to spoofing attacks when compared to using unimodal biometric systems. However, based on the nature of asymmetric encryption, it will increase the overall process time, which makes this proposal slow.

In [15], the issue with using knowledge-based, and physiological-based authentication mechanisms was explained, based on the usage of a mobile phone as a multi-purpose device for different activities. Evidently, the frequency of its usage is high, resulting in an increased frequency of both PIN and password inputs. As a result, employing non-intrusive methods for user authentication seems to be most ideal. For instance, in [16], an accuracy of 90.23% was achieved, using fingerprint and ear pattern captures to identify a user. A training and testing time of 6.07s and 20s were used respectively. This novel biometric user authentication achieved high accuracy levels, justifying its convenience, compared to hardware-based methods.

In [15], "IntelliAuth" was introduced, based on the user's behavioral biometric with the ability to use the environmental sensing to improve the authentication using a proximity sensor. Mobile sensors of accelerometer, gyroscope, and magnetometer are used user authentication. This proposal is novel as the result of the Bayes-Net classifier produced a 97.38% accuracy when compared to the other classifiers (decision tree, K-NN and SVM). The work presented in [16] proposed a multisensory authentication system which continuously authenticates the user. Just like previous work, behavioral biometrics are used, so it does not require direct user involvement. Also, like its predecessor, the method proposed in [16] uses the accelerometer, orientation, and magnetometer sensors.

In addition, the proposal presented in [17] uses the gyroscope and accelerometer sensor to authenticate a user. The preservation of the users data captured from the sensors was considered by implementing a format preserving encryption technique. This was a countermeasure to reduce personal data leaks since most of the authentication systems use machine learning algorithms which are sometimes outsourced to the Cloud, making them be prone to attacks. Despite using cryptography for securing user data, an accuracy of 76.85% was achieved with no significant impact on the authentication process.

In the area of using voice for authentication, researchers in [18] developed a continous authentication system using a fusion of mobile phone sensors and speaker information. This proposal is novel as it is a multimodal form of authentication, similar to the one in [19], which produced high accuracy rate. However, voice recognition has setbacks because it is not convenient to be used by people with learning difficulties, or speech impediments. Also, its accuracy may be compromised if a person's voice changes due to different health and emotional conditions.

In [20], a subystem for continous user identification using mobile phones was introduced. It was based on how they interact with their phones (hand movement and waving patterns). To test the performance of the system, random forest, support vector machine and Bayesian networks were used, reaching an accuracy of 74.9% using the random forest classifier.

In conclusion, the mobile sensor will enhance user authentication for the implementation of transparent authentication for a mobile device. The fusion of several sensors will improve the data available, resulting in an increased accuracy for mobile user authentication.

III. EVALUATION METHOD

This proposed work is to evaluate and analyze the explicit and continuous authentication of mobile phone users. The availability of real-time sensorial data via mobile phone sensors provides useful information to analyze a user's environment, the usage patterns, and user mobility

Using the sensorial data and the computational capabilities of smartphones, the proposed work includes data collection, pre-processing of data, feature extraction, and classification. The details of each step are explained in the following sections.

A. DATA COLLECTION

Data is collected from 30 healthy participants using a third-party application called TOHRC data logger available on the android play store. To create a real-life scenario, participants carried out some activities sitting, standing, walking both on plain floor and staircase, on a platform and walking down a staircase. These activities are used because data was collected in a controlled (University building, individual homes) environment under a short period of time and those activities reflects a person's

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

usual day-day activities. Each of this activity is recorded for thirty (30) seconds with a sampling rate of 50Ghz.

The mobile device was held by the participant while doing all activities. The experiment was carried out using four different activities for each participant. The activities are listed below:

- Activity 1: User sitting for a defined time while the data was collected.
- Activity 2: User standing for a defined time while the data was collected.
- Activity 3: User walking for the duration for a defined time while the data was collected.
- Activity 4: User walking down and up a staircase for a defined time while the data was collected.

B. OVERVIEW OF SENSORS

Mobile phone sensors are categorized into three, this is based on the sensor data type. The sensor categories are

1. Motion sensors
2. Position sensors
3. Environmental sensors

The motion sensors measure acceleration and rotational forces along the X, Y, Z-axis. Examples of motion sensors are the accelerometer, gyroscope, gravity sensors etc.

The position sensors measure the physical position and orientation of the mobile phones. the position sensors include the orientation, proximity, and magnetometer sensors. The environmental sensors are used in measuring environmental parameters. Examples of environmental sensors are thermometers, barometers. For this project, the position and motion sensors were used. Position and motion sensors have shown to be accurate and have been widely used for mobile phone user authentication [21]. The sensors selected in this study are used because they represent useful information about the user's behavior and environment. Based on the research work presented in [16], the accelerometer can detect coarse-grained motion of a user. This can be used for gait recognition while the orientation sensor can be used for analyzing how the user positions the device and the magnetometer is useful for environment representation. A combination of two or more of these sensors with similar functions would enhance mobile user authentication accuracy. The list of the sensor include:

- Accelerometer, linear acceleration sensor and gyroscope
- Orientation, proximity, and magnetometer sensors
- GPS and gravity sensors

TABLE II. SHOWING THE SENSOR AND POSSIBLE FEATURES (REPRESENTS FEATURES THAT CAN BE EXTRACTED FROM THE SENSOR AND – REPRESENTS OTHERWISE)*

Sensors / Feature	Variance	Sum	Maximum	Minimum	Mean	Standard Deviation	Percentile 25	Rootmean square	Peak-Peak	Kurtosis	Skewness
Accelerometer	*	*	*	*	*	*	*	*	*	*	*
Gyroscope	*	*	*	*	*	*	*	*	*	*	*
Line Acceleration	*	*	*	*	*	*	*	*	*	*	*
Gravity-sensor	*	*	*	*	*	*	-	-	-	-	-
Magnetometer	*	*	*	*	*	*	-	-	-	-	-
Rotation-sensor	*	*	-	-	*	*	-	-	-	*	*
Total	6	6	5	5	6	5	3	3	3	4	4

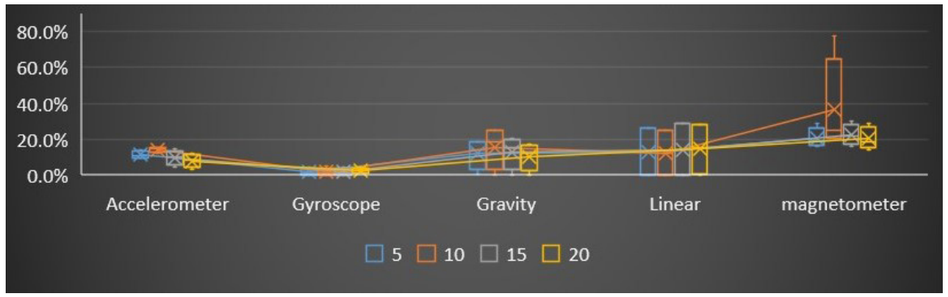
C. NEURAL NETWORK CLASSIFIER

Neural Network is an adaptive system that changes its structure or internal information flow using neuron for training time. This consists of hidden layers, and an output layer in the architecture. The number of neurons used for training the data is useful for determining the accuracy of the overall neural network classification. The number of neurons could be led to either underfitting or overfitting. The underfitting is when few neurons are used in the hidden layer and overfitting is when too many neurons are used for training. To overcome this issue, four different sizes of 5, 10, 15, and 20 network sizes are used to determine the best layer which could be used for each activity. Each of this activity is analyzed per sensor for all the neural network sizes compared.

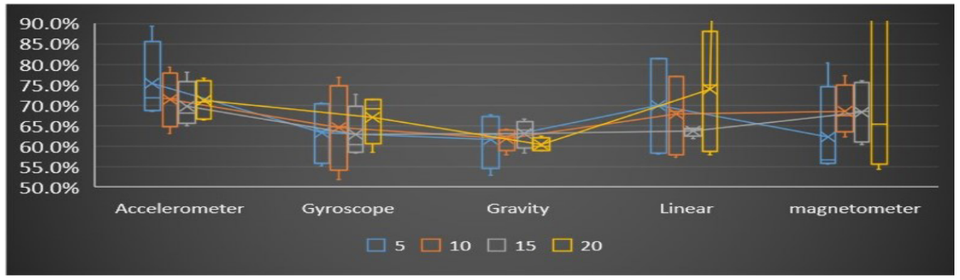
D. EVALUATION METRICS

The research evaluated the proposed method using three (3) metrics widely in biometric authentication, these are:

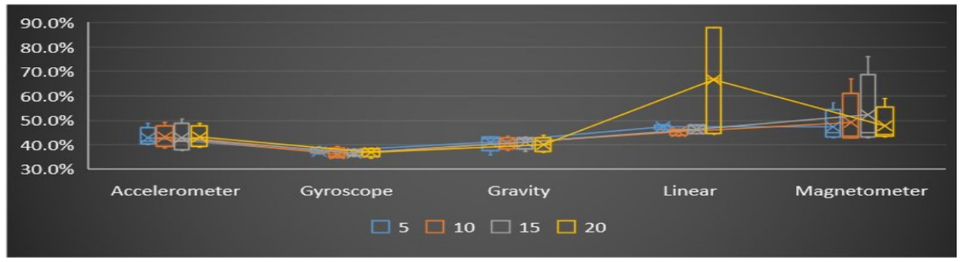
- False Acceptance Rate (FAR) the false identity acceptance of an impostor.
- False Rejection Rate (FRR) is the



(a) Best Individual Performance in EER (%)



(b) Worst Individual Performance in EER (%)



(c) Overall Classification Performance in EER (%)

Fig. 1. Classification Performance

probability that the identity verification system incorrectly rejects the genuine user.

- Equal Error Rate (EER) is the meeting point of the plot of FAR and FRR. The lower the value of ERR, the higher the accuracy of the biometric system.

IV. MULTI-USER EVALUATION

Four network sizes are analyzed for the different sensor while participants carried out activities. This includes network size 5 ,10, 15, and 20.

In Figures 1(a) and 1(b), the best and worst individual performance is shown. Figure 1(c) shows the overall performance of all the classification.

A. INDIVIDUAL PERFORMANCE

The individual performance shows the best as the gyroscope followed by the accelerometer irrespective of the activity.

B. OVERALL PERFORMANCE

The overall performance shows the gyroscope as the best. However, the overall performance in Figure 2 shows that when using a different network size to improve the performance, the accelerometer performed better when a 45-size neural network was used.

V. ENHANCED PERFORMANCE EVALUATION FOR THE SENSORS

To investigate the performance of the sensors,

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

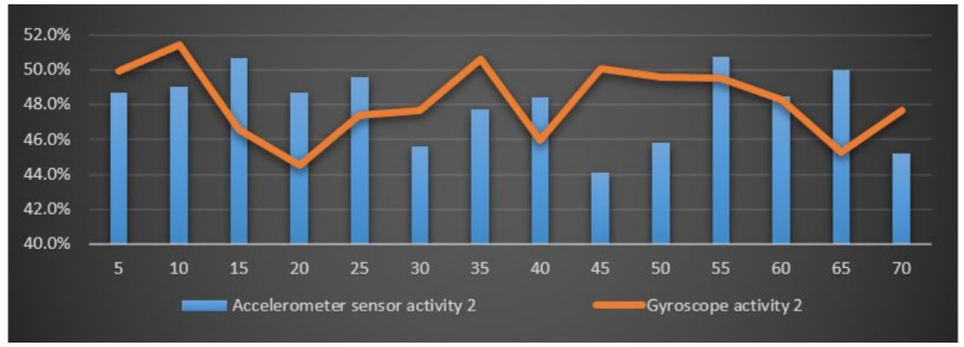
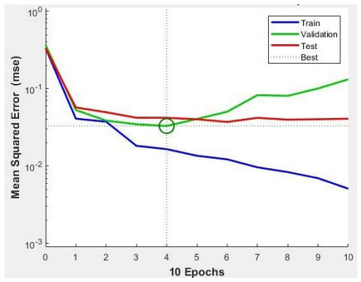
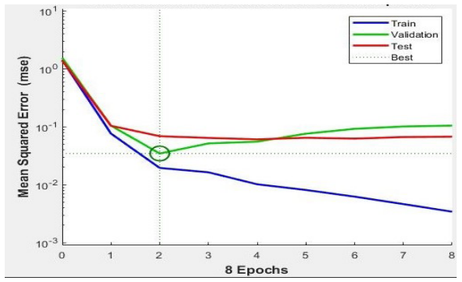


Fig. 2. Overall Performance in EER (%)



a) 0.032946 at epoch 4



b) 0.034672 at epoch 2

Fig. 3. Accelerometer Results for Standing Activity

we evaluate the performance of the sensors using the four activities. The study used the FAR (false acceptance rate) and FRR (false rejection rate). The final output from the two matric gives the EER (equal-error rate) for evaluation and analysis of the result. The EER biometric accuracy measure is used in this research. The most effective biometric control system is the one with the lowest ERR or CER.

The biometric that has the highest EER is the most ineffective. However, it is important to ensure the data is fully trained before analyzing the result.

The neural network training tool is used to train the data showing the data trained and the algorithm used. Mean Square Error (MSE) is used as the performance metric.

Performance has four lines: Trains, test, validation, and best. Performance for each of the training, testing, and validation sets is shown on a log scale. The best line (dotted) confirmed that training of the data had been done successfully. In all the activities, it can be seen decreasing as the data was trained. The network that did best on the validation set was used to calculate the ERR of all activities.

The result of the experiment is explained using tables and graphs.

Table 3 shows the result of standing activity. The lowest EER is 0.26% and the highest is 22.14 percent. Figure 3a) and 3b) shows the neural network training performance curve, and the best validation performance for sitting activity is 0.032946 at epoch 4.

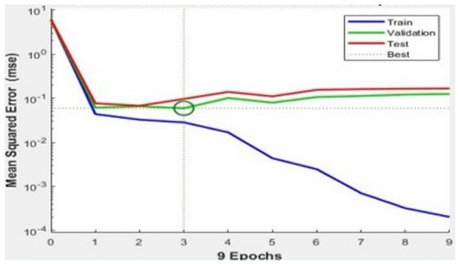
TABLE III. EER IN STANDING ACTIVITY

Activity	*Lowest EER*	*Highest EER*	*Overall EER*
Standing	*0.26%*	*22.14%*	*6.55%*

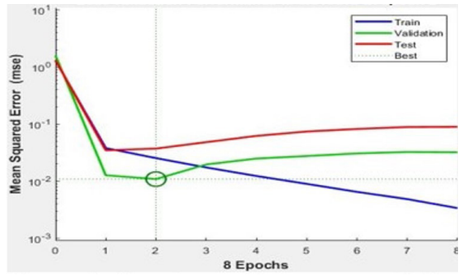
Table 4 below gives information about sitting activity. Sitting activity result achieved the lowest EER of 0.26%, and the highest EER of 32.49%. The overall ERR of this activity is 10.16%.

TABLE IV: EER IN SITTING ACTIVITY

Activity	*Lowest EER*	*Highest EER*	*Overall EER*
Sit	*0.26%*	*32.49%*	*10.16%*



a) 0.05942 at epoch 3 for walking activity



b) 0.010879 at epoch 2 for stair activity

Fig. 4. Accelerometer Results for Walking and Stair Activity

Fig. 5. All-Activity EER Performance of the Accelerometer

Figure 4a) shows neural network training performance curve, and the best validation performance for walking activity is 0.05942 at epoch 3.

TABLE V. EER IN WALKING ACTIVITY

Activity	*Lowest EER*	*Highest EER*	*Overall EER*
Walking	*10.06%*	*54.77%*	*38.11%*

Figure 4b) shows neural network training performance curve, and the best validation performance for stair activity is 0.010879 at epoch 2. As the Table 6 below indicates, the lowest EER of 13.53% was achieved. The highest EER is 54.55%. The table also shows the overall EER for stair activity is 38.77%.

TABLE VI. EER IN STAIR ACTIVITY

Activity	*No of Features*	*Lowest EER*	*Highest EER*	*Overall EER*
Stairs	*30*	*13.53%*	*54.55%*	*38.77%*

In Figure 5, we use three indicators to describe the overall EER for all activities of the accelerometer sensor. To begin, standing activity has the lowest EER amongst all activities. standing activity (act. 1) has the lowest EER of 6.55%. Then followed by sitting activity (act. 2), which has an EER of 10.16%. The other two activities have an ERR that is significantly high when compared to the first two.

The overall EER of activities walking (act. 3) and walking up and down the stairs (act. 4) are also shown, with act. 3 having the overall EER of 28.11% and act. 4 having 38.77%. The most effective biometric control system is the one with the lowest ERR. The lowest EER of the accelerometer sensor is 6.55%, which means the experiment achieved 93.45% accuracy rate of authenticating the user. The highest EER is the most ineffective, which is 38.77%; this means it has 61.23% accuracy rate of authenticating a user.

VI. DISCUSSION AND FUTURE WORK

This research utilized a dataset of 30 healthy participants (users). The research examined the performance of multiple sensors across four activities: stand, sit, walk, and stairs. The signals (data) extracted from the three sensors of accelerometer, gyroscope, and magnetometer attributed to a larger feature vector which shows that the mobile sensor can be used for active authentication. Using the EER for evaluating the result, the higher the EER value, the lower the accuracy, on the other hand, the lower the EER value, the higher the accuracy of the biometric system [22].

In each activity the difference in the highest and lowest EER is significant because data was collected for 30 seconds. Future work would investigate collecting data for a longer period while users carry out different day-day activities.

In comparison with existing literature presented in the literature review, this research achieved a better performance than some of the existing studies. In [23] for example, a biometrics authentication mechanism using motion sensor of a smartphone was presented. The experiment was performed with the mobile user holding the mobile and moving around to perform a signature. The accelerometer used for the motion pattern detection. The result of the experiment confirmed that a single sensor can be used for authentication purposes. The study also demonstrated how a single sensor could be used for authentication purposes. The experiment achieved a false accept rate (FAR) of 1.46% and false rejection rate (FAR) of 6.87%, which has a better performance than the performance our experiment, which achieved an equal error rate (EER) of 6.55% and 10.16%. However, in [23], researchers developed an application that was explicitly used to gather only the necessary data for user authentication, whereas a third-party application was used in this research. In addition to that, [23] utilized only 6 participants for their experiments. Having more participants in our experiments, it was easier to distinct users and have better results with enhanced biometric performance.

REFERENCES

[1] S. Balakrishna, M. Thirumaran and K. V. Solanki, “A Framework for IoT Sensor Data Acquisition and Analysis,” EAI Endorsed Transactions on Internet of Things, vol. 4, no. 16, 2018.

[2] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth and A. J. AviG, “This pin can be easily guessed: Analyzing the security of smartphone unlock pins,” IEEE Symposium on Security and Privacy (SP), pp. 286-303, 2020.

[3] N. Chakraborty and S. Mondal, “Color Pass: An intelligent user interface to resist shoulder surfing attack,” in Proceedings of the 2014 IEEE Students’ Technology Symposium, 2014.

[4] C. Shen, Y. Li, Y. Chen, X. Guan and R. A. Maxion, “Performance analysis of multi-motion sensor behavior for active smartphone authentication,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 48-62, 2017.

[5] M. Muaaz, “A Transparent and Continuous Biometric Authentication Framework for User-Friendly Secure Mobile Environments,” UbiComp, pp. 4-7, 2013.

[6] C. Giuffrida, K. Majdanik, M. Conti and H. & Bos, “I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics,” Proceedings of the 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), pp. 92-111, 2014.

[7] C. Nickel, T. Wirtl and C. Busch, “Authentication of smartphone users based on the way they walk using k-nn algorithm.,” Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 16-20, 2012.

[8] G. Savedna and M. Haryana, “Biometrics in Mobile Security,” International Journal of Mobile & Adhoc Network, vol. 1, no. 1, pp. 14-17, 2011.

[9] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, “A fingerprint and finger-vein based cancelable multi-biometric system,” Pattern Recognition, vol. 78, pp. 242-251, 2018.

[10] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov and J. Yearwood, “Protection of privacy in biometric data,” IEEE Access, vol. 4, pp. 880-892, 2016.

[11] A. K. Trivedi, D. M. Thounaojam and S. Pal, “A robust and non-invertible fingerprint template for fingerprint matching system,” Forensic Science International, vol. 288, pp. 256-265, 2018.

[12] R. Purkait, “External Ear: An analysis of its uniqueness,” Egyptian Journal of Forensic Sciences, vol. 6, no. 2, pp. 99-107, 2016.

[13] C. Lin and A. Kumar, “Contactless and partial 3D fingerprint recognition using multi-view deep representation,” Pattern Recognition, vol. 83, pp. 314-327, 2018.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

[14] D. Jagadiswarya and D. Saraswady, “Biometric Authentication using Fused Multimodal Biometric,” Procedia Computer Science, vol. 85, pp. 109-116, 2016.

[15] M. Ehatisham-ul-Haq, M. A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem and Y. Amin, “Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing,” Sensors, vol. 17, no. 9, pp. 1-31, 2017.

[16] W.-H. Lee and R. B. Lee, “Multi sensor authentication to improve smartphone security,” International Conference on Information Systems Security and Privacy (ICISSP), pp. 5-30, 2016.

[17] L. Hernandez-Alvarez, J. M. de Fuentes and L. González-Manzano, “SmartCAMPP - Smartphone-based continuous authentication leveraging motion sensors with privacy preservation,” Pattern Recognition Letters, vol. 147, pp. 189-196, 2021.

[18] J. M. Espín López, A. Huertas Celdrán, J. G. Marín-Blázquez, F. Esquembre and G. Martínez Pérez, “S3: An AI-Enabled User Continuous Authentication for Smartphones Based on Sensors, Statistics and Speaker Information,” Sensors, vol. 21, no. 11, p. 3765, 2021.

[19] M. Gomez-Barrero, J. Galbally and J. Fierrez, “Efficient Software attack on multimodal biometric systems and its application to face and iris fussion,” Pattern Recognition letters, vol. 36, pp. 243-253, 2014.

[20] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. E. U. Haq and M. A. Azam, “Identifying smartphone users based on how they interact with their phones,” Human-centric Computing and Information Sciences, vol. 10, no. 7, 2020.

[21] A. Buriro, “Behavioral Biometrics for Smartphone user authentication,” International Doctoral School in Information Engineering and Communication Technologies (ICT), Italy, 2017.

[22] R. D. Newbold, Newbold’s Biometric Dictionary: For Military and Industry, Bloomington: AuthorHouse, 2008.

[23] A. Laghari and Z. A. Memon, “Biometric authentication technique using smartphone sensor,” 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 381-384, 2016.

[24] I. Papavasileiou, Z. Qiao, C. Zhang, W. Zhang, J. Bi and S. Han, “GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors,” Smart Health, vol. 19, pp. 1-18, 2021.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

AUTHORS

Eniola Adewumi

I am currently a PhD. Student since 2021 and graduate teaching assistant at Sheffield Hallam University. I previously studied an MSc in Information System Security at Sheffield Hallam University and a BSc in Computer Science at University of Jos Nigeria.
Over the years I have developed great interest in Authentication and have worked and I am still working on methods for mobile phone and Internet of things (IOT) authentication. I also have great interest in Machine learning algorithms.
My current research is an analysis of Heart rate Variability for authentication ad wellbeing assessment.

Timibloudi Enamamu

Dr. Enamamu received his BSc in Communications Systems from the London Metropolitan University in 2009 and his MSc in Telecommunication Engineering from Middlesex University in 2012, and a Ph.D. degree in Electronics and Communication Engineering in 2019 from the University of Plymouth all in the UK. He is a lecturer in the Department of Computing, Sheffield Hallam University, Sheffield, U.K. His research interests include mobile security, transparent authentication, m-health data security, and biometrics. Dr. Enamamu is a member of the IEEE. He is a reviewer for IEEE Access and MDPI Sensor Journals.

Aliyu Dahiru

E. Adewumi, T. Enamamu, A. Dahiru
"Performance Evaluation of Mobile Sensor for Context Awareness User Authentication",
Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763156

Automatización Web del Proceso de Votación de las Elecciones de la EPN Utilizando Esquema de Seguridad de Firma Ciega

Web Automation of EPN's Electoral Voting Process Using Blind Signature Security Scheme

ARTICLE HISTORY

Received 24 March 2022
Accepted 02 May 2022

Jose Azadobay
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
jose.azadobay@epn.edu.ec

Michael Morales
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
michael.morales@epn.edu.ec

Hernán Ordoñez
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
hernan.ordonez@epn.edu.ec

Carlos Montenegro
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
carlos.montenegro@epn.edu.ec

Automatización Web del Proceso de Votación de las Elecciones de la EPN Utilizando Esquema de Seguridad de Firma Ciega

Web Automation of EPN's Electoral Voting Process Using Blind Signature Security Scheme

Jose Azadobay
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
jose.azadobay@epn.edu.ec

Michael Morales
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
michael.morales@epn.edu.ec

Hernán Ordoñez
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
hernan.ordonez@epn.edu.ec

Carlos Montenegro
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
carlos.montenegro@epn.edu.ec

Resumen— En la actualidad, la Escuela Politécnica Nacional tiene un proceso electoral que se lo realiza de manera manual. Por lo tanto, representa un trabajo de gestión considerable a la hora de ser llevado a cabo. Además, dada la naturaleza de los procesos manuales, está sujeto a errores humanos. Como solución a estas y otras problemáticas, el presente trabajo plantea su automatización a través de un sistema web de votación electrónica. El sistema propuesto implementa un esquema de seguridad de firmado ciego, para controlar tanto la privacidad como la validez de los votos. El desarrollo se lo realizó bajo el marco de trabajo de Scrum, debido a su ajuste a equipos de desarrollo pequeños y a su enfoque en la entrega de software funcional en cortos periodos de tiempo. El sistema implementa una arquitectura Modelo-Vista-Controlador, teniendo el desarrollo de la vista en Angular; el controlador en la plataforma .NET Framework y, finalmente, el modelo en SQL Server. Por otra parte, el sistema ha sido sometido a pruebas de usabilidad y funcionalidad, con lo que se determinó que es óptimamente usable y cumple satisfactoriamente con el 100 % de los requisitos de usuario obtenidos.

Palabras Clave— Votación Electrónica, Firma Ciega, RSA, Scrum

Abstract—Currently, the Escuela Politécnica Nacional has an electoral process that is done manually. Therefore, it represents a considerable management work when it comes to being carried out. Also, given the nature of manual processes, it is subject to human errors. As a solution to these and other problems of the electoral process in force in the institution, the present work proposes its automation through an electronic voting system. The proposed system implements a blind signing security scheme to control both the privacy of the voter and the validity of the votes. The development was carried out under the Scrum framework, due to its adaptation to small development teams and its focus on delivering functional software in short periods of time. The system implements a Model-View-Controller architecture, having the development of the view in the JavaScript framework, Angular, the controller in Microsoft .NET Framework and finally the model in SQL Server. On the other hand, the system has been subjected to usability and functionality tests, so it was determined that it is optimally usable and satisfactorily meets 100% of the user requirements obtained.

Keywords— Electronic Voting, Blind Signing, RSA, Scrum

I. INTRODUCCIÓN

Con el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), el sistema educativo nacional y global ha tenido grandes cambios, de los cuales, el tecnológico ha sido uno de los más representativos [1]. Estos cambios implican nuevas formas de preparar, adquirir y transmitir la información [2].

A pesar del crecimiento del uso de las TIC, existen procesos en los cuales no han tenido el impacto esperado, como lo es el caso de la gestión de procesos electorales [3]. El proceso electoral que actualmente rige en la mayoría de las instituciones de educación superior y específicamente en la Escuela Politécnica Nacional (EPN), se lo realiza de manera manual, por lo tanto, está expuesto a fallas de tipo humano.

El desarrollo de un sistema de votación electrónica, que permita la ejecución más eficiente del proceso electoral de la EPN, contribuirá en la disminución de los factores del error humano y los tiempos en la obtención de resultados. Además, aporta positivamente a la preservación del ambiente ya que se elimina el uso de papeletas físicas.

El objetivo principal del presente trabajo es automatizar el proceso de votación de las elecciones de la EPN a través de un sistema de votación electrónica, con el fin de mejorar sustancialmente su desempeño.

Con el fin de garantizar el anonimato y la integridad del voto en el sistema propuesto, se implementa un esquema de firmado ciego, el cual se basa en tener una entidad independiente que se encargue de certificar la validez de un voto, sin necesidad de conocer la identidad del votante. De esta manera, se tiene un voto certificado y anónimo.

El aplicativo web del sistema propuesto está desarrollado en la versión 10 del framework de JavaScript, Angular. La lógica del sistema está implementada bajo la plataforma .Net de Microsoft y bajo esta misma plataforma se maneja la comunicación entre el aplicativo web y la lógica del negocio. Además, el sistema está construido bajo el marco de trabajo de desarrollo ágil, SCRUM.

A. SITUACIÓN ACTUAL

Actualmente, los procesos electorales en la EPN se los conlleva de la manera tradicional, es decir, son netamente manuales. Todo el proceso requiere del compromiso de un contingente humano desde la organización y designación de la Junta electoral hasta el final del proceso con la proclamación de resultados [4].

De acuerdo con el último estatuto de la EPN reformado el 24 de octubre de 2019 [5], la institución está estructurada, a nivel directivo, por:

- Consejo Politécnico
- Consejo de Docencia
- Consejo de Investigación, Innovación y Vinculación
- Consejos de Facultad
- Consejos de Instituto
- Consejos de Departamento
- Consejo Directivo de la Escuela de Formación de Tecnólogos

B. ALCANCE

El presente proyecto se llevará a cabo con base en ciertos puntos tomados de la ISO/TS 54001:2019. La norma comprende 8 subprocesos que garantizan el correcto desempeño de un organismo electoral [6], estos son:

- Inscripción electoral
- Inscripción de organizaciones políticas y de candidatos
- Logística electoral
- Emisión del voto
- Escrutinio y declaración de resultados
- Educación electoral
- Fiscalización del financiamiento de campañas electorales
- Resolución de conflictos electorales

De los subprocesos mencionados anteriormente, el sistema a implementar ayuda con la automatización de la emisión del voto y, el escrutinio y declaración de resultados. Cabe mencionar que el sistema únicamente emitirá los resultados obtenidos en el proceso de escrutinio, mismos que deberán ser necesariamente analizados por el personal miembro de junta para su respectiva declaración. Además, el sistema ayudará en parte al subproceso de logística electoral.

El subproceso de emisión del voto establecido en esta ISO, menciona que el voto deberá ser secreto, por tanto, para cumplir con este punto, se ha optado por la solución tecnológica del firmado ciego, el cual será detallado más adelante en el documento.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

C. METODOLOGÍA

Para la parte del desarrollo de la aplicación web, se utilizará la metodología ágil de desarrollo SCRUM, por ser un marco de trabajo que permite automatizar procesos que pueden llegar a ser complicados [7]. Este es el caso, puesto que el desarrollo de un sistema de voto electrónico puede llegar a tener un nivel de complejidad elevado ya que se debe garantizar la seguridad durante todo el ciclo de vida del proyecto, debe ser robusto, transparente y eficiente. Se utilizarán varias técnicas como patrones de diseño y técnicas de seguridad de datos a nivel de aplicación.

El grupo de trabajo que llevará a cabo la realización del proyecto propuesto en este documento está conformado por cuatro personas. Por tanto, al ser un grupo pequeño, SCRUM es de gran utilidad ya que este se enfoca principalmente en el desarrollo de proyectos que conlleva un recurso humano relativamente pequeño y manejable no mayor a 8 personas [8].

Además, gracias a la experiencia compartida en la implementación de sistemas similares [9], se puede confirmar que el uso de la metodología Scrum, resulta favorable para el desarrollo del sistema propuesto en el presente documento, ya que permite un manejo apropiado de las expectativas del cliente, basado en resultados tangibles.

D. HERRAMIENTAS

El proyecto descrito en este documento utiliza una arquitectura de tres capas utilizando el patrón de diseño Modelo Vista Controlador (MVC), el cual es un patrón de diseño de software que separa los componentes de aplicación en tres niveles: Modelos o base de datos, Vista o aspecto visual y controlador o lógica. En los cuales, cada uno de ellos tiene responsabilidades específicas [10]. La arquitectura se la puede observar en la Figura 1.

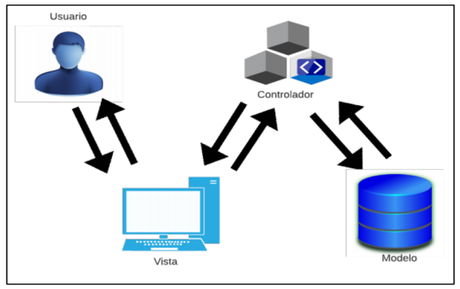


Fig. 1. Arquitectura del sistema

E. ESQUEMA DE SEGURIDAD DE FIRMA CIEGA

La firma digital, introducida inicialmente por Chaum [11], se utilizó en un principio para diseñar el primer protocolo de dinero electrónico. Posteriormente, se utilizó para verificar los votos en los esquemas de votación electrónica. Una firma digital estándar debe proporcionar ciertas características para garantizar comunicaciones digitales fiables:

- Autenticación: Todo el mundo puede verificar a la entidad u origen de la firma digital.
- Integridad: El mensaje recibido ya firmado es exactamente igual al mensaje enviado.
- No repudio: El firmante no puede negar ser el autor de un mensaje firmado válido y verificado.

En un proceso de firma digital ciega participan dos usuarios, el firmante y el cliente. El firmante firma el mensaje y lo cifra con su clave privada, por lo que él es el único que puede generarlo. El destinatario del mensaje puede verificar fácilmente la firma utilizando la clave pública del firmante. Del mismo modo, el firmante no puede negar la firma, porque si esta se puede verificar con su clave pública, significa que la firma ha sido generada con la clave privada que solo el firmante conoce [12]. Mediante el uso de firmas digitales ciegas, una institución autorizada puede firmar digitalmente una serie de datos (por ejemplo, votos) sin conocer el contenido de los datos.

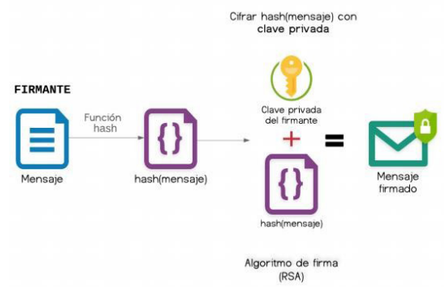


Fig. 2. Proceso de firma ciega

Por otra parte, el receptor puede verificar la firma con la clave pública del emisor o firmante de la siguiente manera:

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

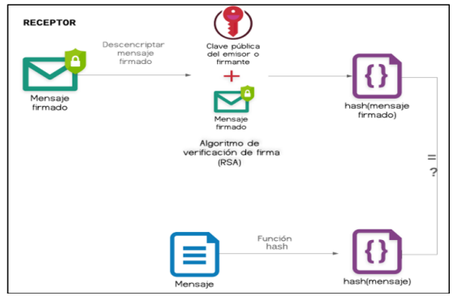


Fig. 3. Verificación de la firma

II. ANÁLISIS Y DISEÑO

A. REQUISITOS DEL SISTEMA

Para el levantamiento de los requisitos del sistema, se ha llevado a cabo entrevistas con miembros de la Federación de Estudiantes de la Escuela Politécnica Nacional (FEPON) y representantes de asociaciones de estudiantes de varias facultades. De las cuales se ha podido determinar los siguientes requerimientos:

- Ingresar al sistema con usuario y clave
- Gestionar diferentes tipos de elecciones
- Gestionar elecciones
- Gestionar escaños
- Configurar postulantes a cargos
- Configurar listas de candidatos
- Configurar procesos electorales
- Importar padrón por proceso electoral
- Enviar mails masivos a los usuarios nuevos
- Gestionar usuarios y personas
- Emitir voto
- Consultar validez del voto

B. MÓDULOS DEL SISTEMA

Con base en los requerimientos obtenidos en las entrevistas con los interesados, el sistema se dividió en cuatro módulos principales listados a continuación:

- Módulo de Configuración
- Módulo de Procesos
- Módulo de Elecciones
- Módulo de Resultados

C. DISEÑO DE INTERFAZ

Para las interfaces del módulo de configuración, se tendrá un estándar. En la parte superior, la ruta de la pantalla en donde se encuentra, esto servirá para que el usuario se ubique de mejor manera en el sistema. Seguido, se tendrá un cuadro de búsqueda, en el cual se podrán buscar registros según parámetros importantes de cada entidad.

Estas pantallas también tendrán un botón para crear nuevos registros, el cual abrirá otra pantalla auxiliar con los campos respectivos de cada entidad, el usuario deberá llenar los campos y guardar el nuevo registro. En las columnas de la tabla se tendrán botones de acción sea para eliminar, editar los registros algún otro tipo de acción implementado.

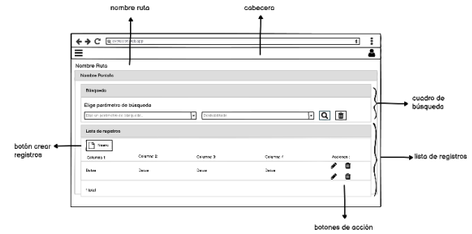


Fig. 4. Mockup de catálogos del sistema

D. ARQUITECTURA DEL VOTO PROPUESTO

La arquitectura propuesta para el proceso de emisión de voto consta de cinco fases y tres entidades participantes: el elector, un esquema de identificación (EI) y otro de votación (EV) como se puede observar en la Figura 5. Además, se considera que los canales de comunicación para el proceso son seguros. En la primera fase, una vez que el elector genera su voto (v) la aplicación, del lado del cliente, lo encripta con AES y genera una máscara (m) mediante una función hash del voto ya cifrado.

Luego, se envía el voto encriptado, la máscara generada, y el token de identificación del elector al llamado esquema de identificación. Este proceso se lo realiza a nivel del backend, en primer lugar, se verifica si el usuario está habilitado para votar, es decir, que aún no haya votado y que conste dentro del padrón electoral.

Si es así, se procede a firmar el voto cifrado + la máscara y se envía este voto firmado F(v',m) al elector. En esta parte, es donde se utiliza el concepto de firma ciega ya que la entidad que firma el voto no conoce realmente lo que está firmando pues el contenido del voto está cifrado y concatenado a una máscara.

Una vez que el elector fue autorizado para votar y ha recibido su voto firmado, lo envía al esquema de votación junto con la máscara, el voto cifrado y la llave utilizada para cifrar/descifrar el voto (keyAES). En el esquema de votación primero se verifica la validez de la firma digital utilizando la llave pública del esquema de identificación y el algoritmo de descifrado RSA explicado en apartados anteriores. Si la firma es válida, quiere decir que tanto el voto cifrado como la máscara no han sido alterados, entonces se procede a descifrar el voto con la ayuda de la llave AES que ha sido enviada desde el lado del cliente.

Una vez que tiene el voto descifrado, se almacenan las opciones que hayan sido elegidas y la máscara. La máscara sirve como identificador único de voto ya que solo es conocida por el elector y almacenada en este único caso. Cabe mencionar que de ninguna manera se puede vincular al elector con el voto o con la máscara debido a que en este instante no se tiene alguna información del elector.

Finalmente, se envía un mensaje de que el voto fue exitoso y el elector guarda su máscara para poder verificar que su voto no haya sido alterado. La verificación del voto se la podrá hacer en cualquier momento luego de que la elección haya finalizado.

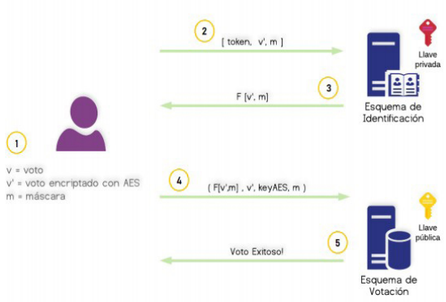


Fig. 5. Arquitectura de voto propuesto

III. IMPLEMENTACION Y PRUEBAS

A. ARQUITECTURA WEB DEL SISTEMA

Como ya se ha mencionado, la arquitectura seleccionada para este sistema está basada en MVC (modelo-vista- controlador). Para el modelo se ha utilizado como gestor de base de datos SQL Server. El controlador se desarrolló utilizando el framework .Net y el lenguaje de programación C#. Para el desarrollo de las vistas y aplicativo web, que se muestra al usuario final, se utilizó el framework Angular en su versión 10. En la Figura 6, se puede observar un resumen de la arquitectura que se detalla más adelante.

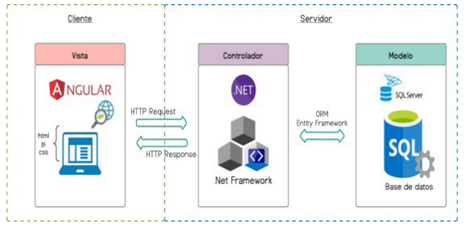


Fig. 6. Arquitectura MVC del sistema

B. MODELO

Para la implementación del modelo, se utilizó un ORM (Object Relational Mapping) llamado Entity Framework que es compatible con el ambiente de trabajo utilizado (.NET). Este ORM permite utilizar objetos de clase específicos para procesar datos sin tener que prestar atención a las tablas y columnas de la base de datos donde se almacenan.

Para este proyecto se trabajó con el gestor de base de datos SQL Server. En la Figura 7, se puede observar cierta parte del modelo de datos la cual representa la estructura de un proceso electoral.

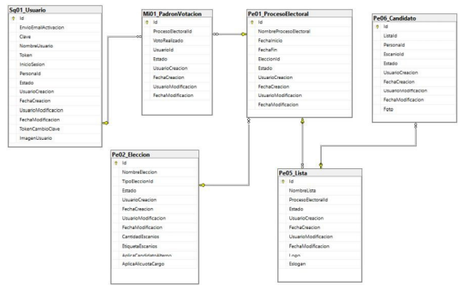


Fig. 7. Modelo físico de la base de datos

C. VISTA

Para la implementación de las vistas del aplicativo web se ha utilizado Angular como framework de desarrollo. Con esta herramienta se puede separar en archivos la parte del código, HTML, y estilos. El sistema cuenta con una pantalla de Login para el inicio de sesión de los usuarios del sistema. Una vez que el usuario inicia sesión exitosamente podrá observar la pantalla de bienvenida que junto con las demás pantallas tienen en común un menú lateral en la parte izquierda donde se encuentra la imagen del usuario, el nombre y las rutas de menú permitidas para cada usuario. También cuenta con una cabecera en donde está la imagen del usuario y un botón para poder abrir o cerrar el menú, y, por último, en el centro se tiene un área que irá cambiando, dependiendo de la ruta a la que se dirige el usuario.

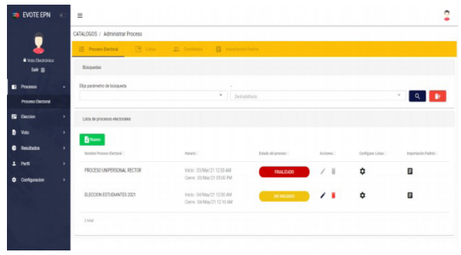


Fig. 8. Pantalla de configuración de procesos.

D. CONTROLADOR

El controlador de la aplicación se ha implementado bajo el framework de .Net y con el lenguaje de programación C#.

Con estas herramientas se ha desarrollado el backend a manera de capas. La capa más interna es la de acceso a datos, en la cual se tienen las entidades y los diferentes métodos para acceder a la base de datos. Cabe mencionar que para las funciones de acceso a datos se ha implementado el patrón repositorio. Con este patrón se crea una sola vez cada método de acceso para que puedan ser utilizados por cualquier entidad.

Luego, se encuentra la capa de lógica de negocio, que viene a ser la capa intermedia entre la capa web API y el acceso a datos. En esta capa, se han implementado todas las reglas de negocio, operaciones con entidades, validaciones, consultas etc. Como resultado se tiene un conjunto de servicios que son expuestos a las capas superiores.

La capa web API es la encargada de recibir las peticiones http y comunicarse con algún servicio para devolver la información requerida por el lado del cliente. En esta capa, se han implementado técnicas de seguridad como la autenticación por token, es decir, si una petición no tiene un token válido, generado por el sistema, no se permite el paso a una capa más interna y se retorna una respuesta de acceso no autorizado. Un ejemplo de controlador a nivel de esta capa se lo puede observar en la Figura 9.

```
[HttpPost]
[Route("VESLPrcCtv")]
public HttpResponseMessage VESLPrcCtv()
{
    try
    {
        var token = Request.Headers.Authorization.Parameter;
        _tokenValidator.ValidarToken(token);
        return Request.CreateResponse(HttpStatusCode.OK, _procesoElectoralService.ObtenerTodosProcesosElectoralesActivos());
    }
    catch (Exception ex)
    {
        return Request.CreateResponse(HttpStatusCode.BadRequest, _apiResponseMessage.crearOtoErrorExceptionMessage(ex));
    }
}
```

Fig. 9. Servicio de obtención de procesos

E. GENERACIÓN DEL VOTO

Una vez que el elector ha seleccionado sus opciones, en caso de que el voto sea válido, se tiene un conjunto de datos de tipo Json con la información necesaria para poder guardar el voto. En caso de que los votos sean de tipo nulo o blanco, el voto se tratará como un arreglo vacío. Después de que el elector verifica su voto y da clic en el botón "Emitir voto", la aplicación web en el lado del cliente procede con el cifrado del mismo para posteriormente enviarlo.

Para el cifrado, lo primero que se hace es generar una llave simétrica que será utilizada para encriptar el voto con el algoritmo AES. Para realizar este cifrado se ha utilizado la biblioteca CryptoJS la cual abarca una gran colección de algoritmos criptográficos estándar y seguros. Por temas de implementación se ha elegido generar también un vector de inicialización (IV) de 16 bytes junto con la llave (keyAES) de 32 bytes. Para la generación de estas llaves se ha desarrollado en el sistema una función, la cual recibe una longitud de cadena y selecciona de forma aleatoria carácter por carácter, de entre un conjunto de caracteres alfanuméricos, para obtener cada llave.

Una vez que tiene el vector de inicialización y la llave AES se las envía junto con el voto en texto plano a la función de encriptación. En esta función, se convierten el par de llaves a formato UTF8 ya que es un requisito de la librería. Luego se hace uso de la función "CryptoJS.AES.encrypt()" adjuntando el par de llaves ya convertidas y el voto. Esta función retornará el voto ya cifrado con el algoritmo AES. En la Figura 10 se detalla dicha función.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

```
encriptarVotoConAes(voto, key,iv) {
        var votoString = JSON.stringify(voto);
        var keyUTF8 = CryptoJS.enc.Utf8.parse(key);
        var ivUTF8 = CryptoJS.enc.Utf8.parse(iv);
        var cifradoAES = CryptoJS.AES.encrypt(CryptoJS.enc.Utf8.parse(votoString), keyUTF8, {
            iv: ivUTF8,
            mode: CryptoJS.mode.CBC,
            padding: CryptoJS.pad.Pkcs7
        });

        return cifradoAES;
    }
```

Fig. 10. Encriptación de voto con AES

Siguiendo la arquitectura de voto propuesto, una vez que se tiene el voto cifrado se procede con la generación de una máscara única para cada voto. Esta máscara ayudará para posteriormente guardar el voto sin tener que asociarlo directamente con el elector. Además, el elector será el único conocedor de su máscara con la cual también podrá comprobar la integridad de su voto.

Para la generación de la máscara se ha usado una función de hash (SHA512) aplicada al voto cifrado y añadiendo ciertos parámetros para brindar aleatoriedad. La estructura de la máscara es SHA-512(t1 | votoAES | t2), donde:

- t1: Instante de tiempo 1 en el cual empieza el proceso de creación de la máscara.
- t2: Instante de tiempo 2 más un valor generado aleatoriamente.
- votoAES: Es el voto cifrado con AES.

F. AUTORIZACIÓN Y FIRMA CIEGA

Una vez que se tiene el voto cifrado y la máscara se procede con el proceso de identificación, autorización y firma ciega del voto. En este instante se realiza la comunicación con el esquema de identificación para lo cual se envía el token de identificación del usuario elector junto el voto cifrado, la máscara generada y un identificador del proceso electoral, codificado en Base64, al cual se desea hacer referencia para el voto.

En el lado del servidor primero se verifica que el usuario conste en el padrón electoral del proceso al cual se está haciendo referencia, que no haya votado aún, que se encuentre dentro del horario habilitado. Si cumple con los requisitos impuestos se autoriza el voto al elector y empieza el proceso de firmado ciego.

Para implementar el proceso de firmado ciego se ha hecho uso de un proveedor de servicios criptográficos "System.Security. Cryptography" desarrollado en C# y que sirve para .Net. Este servicio necesita en primer lugar un par de claves, la pública y la privada, para poder trabajar con el algoritmo RSA.

Una vez con las claves ya generadas, para la firma del voto se utiliza solo la clave privada. Haciendo uso de la biblioteca de criptografía se utiliza la función SignData(); a la cual se le pasa el String cifrado (AES) del voto concatenado con la máscara y codificados en formato UTF8. Luego se especifica el tipo de función hash que se desea utilizar, en este caso SHA512. Esta función devuelve como resultado la firma digital de los datos proporcionada.

```
public string FirmaDigital(string text)
{
    //Transformar el mensage a un array de bits en codificación UTF8
    var encoder = new UTF8Encoding();
    var bytesText = encoder.GetBytes(text);
    // Hash y firmar los datos.
    var signedData = _privateKey.SignData(bytesText, CryptoConfig.MapNameToOID("SHA512"));
    return Convert.ToBase64String(signedData);
}
```

Fig. 11. Servicio de firma digital

G. GUARDADO DEL VOTO

En el lado del cliente cuando ya se ha obtenido la firma digital se procede con el guardado del voto. Para esto se envían la firma digital, el voto cifrado con AES, las respectivas llaves para el descifrado y la máscara. Como se aprecia en esta parte dejamos de lado el token identificador del elector, garantizando el voto secreto, ya que si se cuenta con una firma digital significa que el usuario ha sido autenticado y autorizado.

El esquema o mesa de voto recibe toda esta información necesaria para primero, poder comprobar la validez de la firma. De la misma manera, en este punto se utiliza la función de la librería criptográfica VerifyData(); la cual utiliza la clave pública del esquema de identificación junto con los datos firmados y los datos de origen para verificar la firma.

```
public bool VerificarFirmaDigital(string datosOriginales, string datosFirmados)
{
    var encoder = new UTF8Encoding();
    var datosOriginalesBytes = encoder.GetBytes(datosOriginales);
    var datosFirmadosBytes = Convert.FromBase64String(datosFirmados);

    var decryptedBytes = _publicKey.VerifyData(datosOriginalesBytes, CryptoConfig.MapNameToOID("SHA512"), datosFirmadosBytes);

    return decryptedBytes;
}
```

Fig. 12. Función de verificación de firma digital

Si la verificación es exitosa significa que tanto el voto como la máscara son correctos y no han sido manipulados por lo tanto se procede con el guardado del voto. Se debe recordar que en este punto, el voto que se ha recibido por parte del elector sigue estando cifrado a diferencia que esta vez ya se conoce el valor de la clave y el vector de inicialización. Para la obtención del texto descifrado se ha creado una función la cual recibe los valores de las claves AES y el voto cifrado y devuelve la lista de opciones

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

elegidas por el elector en forma de lista de objetos.

Finalmente, con la lista de opciones ya descifradas más los datos proporcionados por el elector se procede a guardar la información en la base de datos. Para soportar este proceso se crearon dos tablas: la tabla voto y la tabla opción. Si el voto a guardar es un voto válido se guarda primero la máscara y el estado en la tabla voto y se crea un registro por cada opción seleccionada guardándolo en la tabla opción. En caso de que el voto sea de tipo nulo o blanco solamente se guarda un registro en la tabla voto junto con el estado correspondiente.

IV. ANÁLISIS DE RESULTADOS

Luego de haber realizado las pruebas de funcionalidad, para un total de 34 historias de usuario, se pudo constatar que el sistema superó satisfactoriamente cada caso de prueba. Por lo tanto, el sistema presenta, según los requerimientos solicitados, una funcionalidad y completitud del 100 %.

En cuanto a la usabilidad del sistema, luego de realizadas las respectivas encuestas a los usuarios, y realizado el cálculo de los resultados obtenidos mediante la herramienta metodológica SUS; se obtiene una puntuación de 84,5/100. Basándonos en la escala proporcionada para esta metodología, la cual se puede observar en la Figura 13, se concluye que el sistema es excelentemente usable.

Fig. 13. Puntuación de aceptabilidad del SUS

V. CONCLUSIONES

A. CONCLUSIONES

- Se ha desarrollado con éxito un aplicativo web que ayuda a automatizar los procesos electorales de la Escuela Politécnica Nacional. El aplicativo ha sido desarrollado con el objetivo de ser configurable y soportar todos los posibles tipos de procesos electorales que se manejen en la institución, incluyendo las elecciones de Rector y sus respectivos Vicerrectores, elecciones internas de las diferentes facultades, elecciones de representantes ante los diferentes consejos, entre otras.
- Después de analizar los requerimientos obtenidos, se definieron cuatro módulos principales para el sistema: Configuración, Procesos, Elecciones y Resultados, mismos que sirvieron para agrupar las funcionalidades y tener un menú de usuario más organizado. Además, esta modularización ayudó a priorizar de mejor manera los requisitos a desarrollar, facilitando así su planificación.
- Gracias al concepto de firma ciega implementado bajo el algoritmo de RSA se logró crear un esquema para la firma digital de los votos de los electores, garantizando la integridad y el anonimato del voto. Además, gracias a esta implementación se pudo conocer más en profundidad sistemas criptográficos como RSA, AES, SHA, firma digital.
- Mediante pruebas de funcionalidad, se determinó que el sistema se encuentra completamente funcional y cumple satisfactoriamente la totalidad de sus requisitos. Además, del resultado obtenido mediante el cálculo de la usabilidad especificado en la metodología SUS, se concluye que el sistema tiene una facilidad de uso excelentemente aceptable.
- El sistema de votación electrónica fue desplegado en un hosting público para llevar a cabo una simulación de un proceso electoral dentro de la EPN y orientado a un número considerable de usuarios. Mediante la aplicación de encuestas, tras finalizar el proceso electoral, se pudo determinar que los usuarios tuvieron una gran acogida al sistema. Esto se debe a la simplicidad de uso y al diseño amigable de la aplicación web.

B. RECOMENDACIONES

- Para la implementación del sistema se ha desarrollado una arquitectura de voto, en donde se separan mediante esquemas la mesa de identificación de la mesa de votación, aunque, compartiendo recursos como la base datos. Por lo tanto, para una mejora en la implementación del sistema de voto electrónico se recomienda separar la funcionalidad de la mesa de votación en una entidad independiente, tanto en infraestructura como en lógica de negocio. Esto ayudaría a fortalecer el anonimato de los electores, ya que dicha entidad se encargaría únicamente de validar y

almacenar los votos firmados, dejando de lado cualquier relación con los usuarios del sistema.

- El sistema desarrollado se enfocó en ofrecer seguridad a nivel del aplicativo web, asumiendo tanto la seguridad de la base de datos como una infraestructura de comunicación altamente disponible. Por tanto, se marca como pendiente la implementación de comunicaciones redundantes, para aumentar la disponibilidad del sistema y reducir la probabilidad de fallos por errores de infraestructura. Además, al ser un sistema que almacena datos muy sensibles, se recomienda manejar una auditoria a nivel de gestor de base de datos, para evitar posibles intervenciones o manipulación de la información. Con estas mejoras, se espera tener un sistema sumamente seguro en todos los ámbitos.

- Para poder guardar el voto de un elector, se utilizó un método que genera una máscara única a partir de dicho voto. Se realizaron alrededor de diez mil pruebas del método de generación de la máscara, con un mismo voto y cambiando únicamente los instantes uno y dos, teniendo como resultado que en ningún momento se repitió dicha mascara. Aun así, se recomienda la implementación de un mecanismo de vuelta atrás, en donde si una máscara generada se repite, se vuelva al esquema de identificación y se genere otra máscara hasta conseguir una que sea única.

REFERENCIAS

[1] L. Borja y D. Rodriguez, «Propuesta Técnológica para la Sistematización del Proceso de Voto Electoral Estudiante de la Unidad Educativa Particular Dante Alighieri del Distrito 3 de la Ciudad de Guayaquil,» Repositorio Universidad de Guayaquil, 2016. [En línea]. Available: https://rraae.cedia.edu.ec/Record/UG_9c115852f00593e2b70a007749e4bdd7. [Último acceso: 2022].

[2] M. Bautista, A. Martínez y R. Hiracheta, «El Uso de Material Didáctico y las Tecnologías de Información y Comunicación (TIC's) para Mejorar el Alcance Académico,» Ciencia y Tecnología, vol. 14, nº ISSN 1850-0870, pp. 183-194, 2014.

[3] A. Bates y A. Sangra, «La Gestión de la Técnología en la Educación Superior: Estrategias para Transformar la enseñanza y el Aprendizaje,» Barcelona, John Wiley & Sons International Rights, Inc, 2016, p. 15.

[4] Consejo Politécnico, Reglamento General de Elecciones de la Escuela Politécnica Nacional, 2019.

[5] Escuela Politécnica Nacional, Estatuto de la Escuela Politécnica Nacional, 2019.

[6] ISO, La Guía Internacional ISO/TS 54001:2019: Requerimientos Específicos para la Aplicación de la Norma ISO 9001:2015 a Organizaciones Electorales en todos los Niveles de Gobierno, 2019.

[7] Proyectos Ágiles, «Beneficios de Scrum,» [En línea].Available: https://proyectosagiles.org/beneficios-de-scrum/. [Último acceso: 2022].

[8] Scrum, «La Guía de Scrum,» 2013.

[9] L. Cuya, «Aplicación de la Metodología Ágil Scrum en el Desarrollo de un Aplicativo para la Gestión de Observadores Electorales,» 2015. [En línea]. Available: http://repositorio.untels.edu.pe/jspui/bitstream/123456789/322/1/Cuya_Liliana_Trabajo_de_Investigacion_2014.pdf.

[10] MVC, «Servicio de Informática ASP.Net MCV 3 Framework,» [En línea]. Available: https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-%20vistacontrolador-mvc.html.

[11] D. Chaum, «Blind signatures for untraceable payments,» Advances in cryptology, pp. 199-203, 1983.

[12] C. Moreno, «Diseño e implementación de un sistema de voto electrónico,» 2016.

[13] I. Sommerville, Ingeniería del software, Madrid: Pearson Education S.A, 2005.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

AUTHORS

Jose Azadobay

JOSE DANIEL AZADOBAY CUTIOPALA nació en Quito - Ecuador, el 14 de enero de 1996. Se graduó como bachiller en Físico Matemático en la “Colegio Experimental Juan Montalvo”, Quito - Ecuador, en el año 2013. En 2021 se graduó de la Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas obteniendo el título de “Ingeniero en sistemas informáticos y ciencias de la computación”,. Ingeniero de software, proactivo, líder, autodidacta con experiencia en React JS, Angular, .Net, Nest JS, Django, SQL, AWS de aprendizaje rápido y continuo, apasionado por el desarrollo web y todo lo referente a la industria. Durante su experiencia profesional ha trabajado como desarrollador de software destacándose y dominando varios lenguajes como C#, Python, Java, Typescript, Javascript, siendo este último en particular su fuerte. Actualmente trabaja para la representación de Hyundai en Ecuador con el cargo de desarrollador Full Stack, liderando varios proyectos e innovando en tecnologías actuales.

Michael Morales

Estudiante graduado de la facultad de ingeniería de Sistemas de la Escuela Politécnica Nacional en agosto del año 2020. Nacido en Quito – Ecuador en el seno de una familia de clase media. Entre sus mayores intereses profesionales se encuentran el desarrollo de aplicativos web y móviles, enfocado tanto en frontend como en backend y en el diseño de aplicaciones con gran énfasis en la experiencia del usuario final, usabilidad y tendencias de interfaces amigables e inclusivas. Siempre motivado por el avance tecnológico y siempre a la vanguardia de los nuevos paradigmas de programación y desarrollo de software. Practicante incondicional de metodologías de desarrollo ágiles, especialmente Scrum y XP. Padre de un niño y esposo. Amante de los deportes de esfuerzo corporal y de los instrumentos musicales de cuerda y viento. Lector de novelas de Ficción, autobiografías y libros con mensajes protesta, aficionado de las obras del escritor Gabriel García Márquez.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6762958

Hernán Ordoñez

Ingeniero en Sistemas Informáticos y de Computación, en 2014, y Magíster en Software Mención Calidad, en 2018, por la Escuela Politécnica Nacional, Quito, Ecuador. Por varios años docente de la Escuela de Formación de Tecnólogos (ESFOT) de la EPN, y en la actualidad es profesor de la Facultad de Ingeniería de Sistemas (FIS), en la Escuela Politécnica Nacional. Autor y coautor de un sin número de publicaciones de interés orientados a aspectos tecnológicos. Sus intereses de investigación incluyen la creación y gestión de software, y la calidad del software. Practicante incondicional de deportes como el futbol, miembro activo del grupo de seleccionados de la facultad de Ingeniería en Sistemas de la EPN.

Carlos Montenegro

Obtuvo su título de MSc en Informática y Ciencias de la Computación en 2001. Actualmente, es profesor en la Escuela Politécnica Nacional. Además, se desempeña como decano de la facultad de Ingeniería de Sistemas de dicha institución y como CEO del departamento de Ciencias de la computación. También ha sido testigo experto de varios incidentes de seguridad nacional. Entre sus intereses académicos se encuentra el aprendizaje de máquina, minería de datos, inteligencia artificial y la gestión de las TIC. Montenegro es autor y coautor de más de doce publicaciones en sus áreas de interés.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol IX, Issue 2, July 2022

Tecnología educativa para enseñar la lectura labial: un análisis sistematico de la literatura

Educational technology to teach lip reading: a systematic review of the literature

ARTICLE HISTORY

Received 27 January 2022
Accepted 02 May 2022

Evelyn Del Pezo Izaguirre
Facultad de Ingeniería Industrial, Sistemas de Información
Universidad de Guayaquil
Guayaquil, Ecuador
evelyn.delpezoi@ug.edu.ec
ORCID: 0000-0003-1156-7603

María J. Abásolo
Facultad de Informática
Universidad Nacional de La Plata CICPBA
La Plata, Argentina
mjabasolo@lidi.info.unlp.edu.ar
ORCID: 0000-0003-4441-3264

César A. Collazos
Departamento de Sistemas
Universidad del Cauca
Popayán, Cauca, Colombia
ccollazo@unicauca.edu.co
ORCID: 0000-0002-7099-8131

E. Del Pezo , M. Abásolo, C. Collazos, "Tecnología educativa para enseñar la lectura labial: un análisis sistemático de literatura", Latin-American Journal of Computing (LAJC), vol. 9, no. 2, 2022.

Tecnología Educativa para Enseñar la Lectura Labial: Un Análisis Sistemático de Literatura

Educational Technology to Teach Lip Reading: a Systematic Review of the Literature

Evelyn Del Pezo Izaguirre
Facultad de Ingeniería Industrial,
Sistemas de Información
Universidad de Guayaquil
Guayaquil - Ecuador
evelyn.delpezoi@ug.edu.ec
ORCID: 0000-0003-1156-7603

María J. Abásolo
Facultad de Informática
Universidad Nacional de La Plata CICPBA
La Plata - Argentina
mjabasolo@lidi.info.unlp.edu.ar
ORCID: 0000-0003-4441-3264

César A. Collazos
Departamento de Sistemas
Universidad del Cauca
Popayán - Cauca, Colombia
ccollazo@unicauca.edu.co
ORCID: 0000-0002-7099-8131

Resumen— El presente estudio es un análisis sistemático de literatura que identifica la producción de recursos educativos a partir de publicaciones científicas, páginas web y tienda de aplicaciones móviles para la enseñanza de la lectura labial a sordos, enfatizando en las metodologías educativas aplicadas y el uso de la tecnología. Los resultados refieren soluciones tecnológicas apoyadas en elementos audiovisuales y textos, dejando en segundo plano la lengua de señas. El enfoque metodológico aplicado es pasivo, combina medios sincrónicos y asincrónicos, utilizan bajos niveles de gamificación y realidad extendida, demanda conocimiento previo de lectura y escritura para interactuar con las herramientas que se orientan a la práctica de vocabulario o frases. La presencia de aplicaciones móviles es mínima en relación con la cantidad de páginas web y proyectos derivados de producciones científicas para enseñar la lectura labial, en general escasamente mencionan documentación técnica de los proyectos salvo que sean producto de estudios formales de postgrado.

Palabras clave— Lectura labial, palabra complementada, sordos, tecnologías móviles, realidad extendida, metodología educativa, técnicas educativas

Abstract— The present study is a systematic analysis of literature that identifies the production of educational resources from scientific publications, web pages and mobile application store for the teaching of lip reading to the deaf, emphasizing the applied educational methodologies and the use of technology. The results refer to technological solutions supported by audiovisual elements and texts, leaving sign language in the background. The methodological approach applied is passive, combines synchronous and asynchronous media, uses low levels of gamification and extended reality, demands prior knowledge of reading and writing to interact with the tools that are oriented to the practice of vocabulary or phrases. The presence of mobile applications is minimal in relation to the number of web pages and projects derived from scientific productions to teach lip reading, in general they scarcely mention technical documentation of the projects unless they are the product of formal postgraduate studies.

Keywords— Lip reading, cued speech, deaf, mobile technologies, extended reality, educational methodology, educational techniques

I. INTRODUCCIÓN

El uso de las Tecnologías de Información y Comunicación (TIC) como el internet, los dispositivos móviles y la Realidad Extendida (RE) se combinan para crear soluciones tecnológicas que aporten a mejorar la comunicación entre la comunidad sorda y oyente, aprovechando sus características de ubicuidad, portabilidad e interacción entre el mundo real y virtual que ofrecen [1], [2].

La RE permite tener al usuario como actor principal y fortalecer en tiempo real la comprensión visual-auditiva mediante los diferentes conceptos que integra: la Realidad Virtual (RV) experimentando la sensación de estar en un mundo virtual utilizando la tecnología, la Realidad Aumentada (RA) integrando elementos virtuales al entorno real, el reconocimiento de voz y gestos identificados como interfaces multimodales (IM), la combinación de RV y RA, entre otros [3], [4].

La versatilidad y bondades de uso que ofrecen estas tecnologías se integran con las

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

metodologías didácticas y técnicas educativas que se utilizan para canalizar el proceso de enseñanza [5]. Los métodos educativos por el nivel de asimilación de contenido se clasifican en reproductivos o pasivos orientados a reproducir el contenido de forma repetitiva y práctica para la apropiación del conocimiento impartido mientras que, el método activo o productivo promueve el descubrir y crear contenido aplicando sus conocimientos y habilidades [6].

La educación apoyada en el uso de la tecnología permite al docente potenciar sus estrategias educativas tanto dentro como fuera del aula, propiciando escenarios de enseñanza- aprendizaje acordes a las necesidades particulares de sus estudiantes y que respondan a los objetivos que se espera lograr en ellos [7].

[8] indican que la ausencia o el desarrollo tardío de una lengua y no la sordera es lo que limita la capacidad de los individuos sordos para adquirir conocimientos prioritarios, con los cuales no solo poder afrontar la adquisición y desarrollo de la competencia lectora, sino, además, lacomprensión y adaptación al mundo que los rodea. Por eso, es importante buscar fortalecer al lenguaje de señas como primer idioma en las personas no oyentes, tomando como referencia que la realidad del núcleo familiar puede o no ser sumativo al proceso, al estar compuesto por personas oyentes con/sin conocimiento de la lengua de señas, o no oyentes con el dominio de esta, lo que los obliga a aprender más de una herramienta complementaria para poder comunicarse [9].

Cada país tiene adaptado su propio lenguaje de señas, inclusive puede cambiar dentro del mismo entorno geográfico por los modismos propios de regiones y ciudades. En el año 2012, se presenta el Diccionario Oficial de la Lengua de Señas Ecuatoriana, que registra alrededor de 5000 palabras y puede encontrarse en formato impreso, digital e implementado en la web como un apoyo al desarrollo de la comunidad sorda. [10], [11].

La lectura labial o labiofacial es uno de los sistemas de comunicación complementarios a la lengua de señas que utilizan las personas sordas. Consiste en identificar la representación visual del sonido también llamados visemas mientras las personas hablan [12], [13], [14], usualmente se inicia enseñando vocales y consonantes [15], [16] para luego ir integrando sílabas hasta completar las palabras y oraciones. Es preciso recordar que muchos fonemas tienen igual representación visual por lo que, tal conocimiento se integra con el desarrollo de otras habilidades del lector labiofacial como: a) interpretar los gestos de las manos, la cara y la postura corporal, b) su capacidad de síntesis y, c) el conocimiento previo del contexto [17]. La generación de visemas durante una conversación no perdura en el tiempo, por lo que el interlocutor sordo debe usar estrategias de reparación conversacional para recopilar los fragmentos percibidos, sintetizarlos y ser capaz de relacionarlos con el contexto que conoce, procurando ser un receptor activo para eliminar cualquier tipo de ambigüedad que pueda percibir o el vacío de detalles perdidos [18].

La lectura labial se conoce también como lectura labiofacial, lectura del discurso, lectura visual, lectura orofacial, labio lectura entre otros, sin embargo, es importante no confundirla con la palabra complementada o *cued speech* que integra señales con las manos a los visemas mientras se habla con la finalidad de ayudar a reconocer de una manera más sencilla los vocablos. Este sistema está más enfocado a satisfacer la comunicación entre pares sordos al demandar un conocimiento previo de las reglas y señas que contempla [17].

Cada persona sorda es diferente, por lo tanto, optará por utilizar las técnicas de apoyo con la que se sienta más a gusto y las alternará entre sí para evitar fatiga y aburrimiento. Como señalan [19]: el niño sordo realiza de un modo intuitivo la percepción del lenguaje mediante la vista, como medio sustitutivo y complementario a la pérdida de información auditiva.

La adopción de la oralidad difiere en el tipo de usuario sordo, pues si es alguien que inicialmente tenía el sentido de la audición parcial o completo y luego lo perdió, le resulta más sencillo correlacionar la oralidad a partir de la lectura labial porque su lengua materna es el español (que integra vocalización, sonido y palabra), sin embargo, para el sordo nativo (su lengua materna es la lengua de señas), la oralidad se adquiere en una segunda lengua que es el español expresada también en formato escrito, lo que agrega una actividad altamente metalingüística y metacognitiva [20]. Se debe rescatar el hecho de que una persona sorda posee limitantes respecto a la audición más no para hablar, por tanto, la lectura labial presenta dos instancias durante el proceso de enseñanza- aprendizaje, en los primeros niveles de escolarización para aprender la vocalización y pronunciación de las palabras en español y en los grados superiores se convierte en una herramienta complementaria de comunicación, particularmente para tratar con interlocutores oyentes con quienes no siempre se dispone de un intérprete humano o tecnológico como apoyo.

El presente artículo pretende sumar esfuerzos para fortalecer la educación inclusiva en la comunidad sorda, conocer las tecnologías emergentes y metodologías que se utilizan como medio de enseñanza-aprendizaje [21], [22] para posteriormente comprender la metodología de enseñanza de la lectura labial como un sistema alterno de comunicación entre sordos y oyentes.

El documento se organizó de la siguiente manera: la sección 2 explica la metodología empleada para la revisión sistemática de literatura. La sección 3 presenta el análisis y clasificación de las publicaciones. La sección 4 manifiesta los resultados del análisis. La sección 5 expone las conclusiones del trabajo.

II. METODOLOGÍA

La pregunta de investigación que motivó el estudio es ¿existe tecnología educativa para enseñar la lectura labial a sordos?

Para responder esta interrogante y desarrollar el análisis sistemático de literatura, se aplicará una metodología cualitativa-descriptiva transversal, apoyada en el método de análisis de Kitchenham [23], que refiere establecer la pregunta de investigación, para proceder con la búsqueda de publicaciones, las que serán evaluadas aplicando criterios de inclusión-exclusión. La información resultante obtenida de las fuentes bibliográficas se debe categorizar, para poder presentar los resultados y finalmente dar lugar a la discusión.

Las bases de datos bibliográficas consultadas fueron ACM, ERIC, IEEE y SCOPUS, limitando la investigación a artículos en inglés en el periodo 2001 al 2021, aplicando 2 cadenas de búsquedas que combinan palabras claves relacionadas con la pregunta de investigación: a) “lip reading” y b) “cued speech” OR “speechreading”.

Las publicaciones resultantes cumplen con el criterio de inclusión de ser estudios del área de ingeniería, computación y educación. Sin embargo, su proceso de análisis también atendió a los siguientes criterios de exclusión, reportando pocas publicaciones a ser analizadas en el presente estudio.

- Tecnologías de asistencia, de reconocimiento automático de lectura labial (con o sin señales *cued speech*).
- Criterios para el diseño de interfaces enfocadas a lectura de labios o *cued speech*.
- Modelos, métodos, algoritmos de reconocimiento de labios/manos para lectura labial; análisis de estructuras/ patrones de labios o producción del habla; factores del entorno que inciden en la lectura labial o *cued speech*; test para evaluar el desempeño de la lectura labial o *cued speech*.
- Análisis o creación de repositorio de videos para utilizarlos en lectura de labios o *cued speech*.
- Revisiones de literatura, encuestas, artículos de opinión, experimentos varios que no detallan uso de herramienta.
- Estudios con enfoque clínico.
- Publicaciones que están duplicadas, incompletas o que no proporcionen información relevante al estudio realizado.

El resultado de la búsqueda fue de 455 casos para la cadena uno aplicando solo 2 al estudio, para la cadena dos se hallaron 518 artículos de los cuales solo 3 aplicaron, dando un total de 5 publicaciones que se resumen en la tabla 1.

TABLA I. PUBLICACIONES SELECCIONADAS

Fuente	“lip reading”			“cued speech” OR “speech-reading”		
	Encontrados	Cumplen criterios de inclusión	Aplican al estudio	Encontrados	Cumplen criterios de inclusión	Aplican al estudio
ACM	13	13	0	2	2	1
ERIC	8	2	1	191	60	0
IEEE	114	108	1	37	25	0
SCOPUS	320	202	0	288	57	2
Totales	455	325	2	518	144	3

Al centrarse en responder la existencia de tecnología educativa, resulta imperante combinar los escenarios a partir de los cuales tutores (familiares o docentes) o inclusive el interesado (persona sorda) tienen a disposición, como es el internet mediante páginas web y las aplicaciones móviles en sus celulares para la búsqueda de este tipo de recurso educativo.

Con la finalidad de complementar el presente trabajo se incorporó información adicional obtenida a partir de:

a) Revisión de artículos mediante búsquedas sistemáticas en bases de datos indexadas, que contribuyeron a que posteriori los autores desarrollen publicaciones sobre el uso de tecnologías móviles, realidad extendida y metodologías educativas para personas sordas, permitió agregar 2 publicaciones más al análisis.

b) Páginas web que enseñan lectura labial, se buscaron en Google, páginas en inglés y español de las cadenas anteriormente especificadas en este artículo, se revisaron los resultados de las 5 primeras páginas y por cada enlace provisto se examinó el contenido de la página y a su vez los enlaces que referían (internos o externos) y que guardaban relación con el tema (cursos, páginas para aprender lectura labial, libros), esta búsqueda permitió obtener 7 páginas web para ser analizadas.

c) Aplicaciones móviles disponibles en Play Store para Sistemas Operativos Android, considerando que al año 2020 representaron una cuota de mercados de algo más del 84% [24], se buscaron aquellas que enseñen lectura labial, solo se encontraron 2 que aplican a este estudio.

En la Tabla 2 se resumen las cantidades de publicaciones, páginas web y aplicaciones que se analizarán en este trabajo.

TABLA II. CATEGORÍAS DE CLASIFICACIÓN POR EL ENFOQUE

Fuente	Encontrados
Publicaciones	7
Páginas Web	7
Apps Android	2
Totales	**16**

III. CLASIFICACIÓN DE LAS PUBLICACIONES

Al cuestionar si existe tecnología educativa para enseñar la lectura labial a personas sordas, se establecieron criterios de clasificación para verificar requisitos de cumplimiento tanto a nivel académico como tecnológico.

Los criterios C1 a C6 corresponden al enfoque académico, y permiten conocer los métodos y técnicas desde las cuales se enseña la lectura labial, temática, edad y tipo de interlocutor, los que se presentan en la Tabla 3.

TABLA III. CATEGORÍAS DE CLASIFICACIÓN POR EL ENFOQUE ACADÉMICO

C1. Métodos educativos para enseñar la lectura labial

Precisa los métodos de enseñanza-aprendizaje utilizados en las aplicaciones móviles.

A: Activo o productivo, aprendizaje mediante la participación activa y el descubrimiento

R: Reproductivo a pasivo, aprendizaje basado en la repetición del conocimiento

NA: No aplica

C2. Técnica aplicada para enseñar la lectura labial

Especifica la técnica aplicada por el instructor al enseñar la lectura labial

J: Juego serio/gamificación

AV: Análisis de videos

AC: Asociación de conceptos en contextos (reglas nemotécnicas)

FE: Fichas de estudio

CC: Completar contenido de oraciones o palabras

HN: Historias narrativas

PR: Preguntas con respuestas múltiples

RA: Reproducir actividades

DE: Desarrollo de ejercicios

C3. Área temática educativa

Identifica el área de aprendizaje que fortalece el proceso de enseñanza.

V: Vocabulario

P: Palabras como unidades dentro de contextos y de las oraciones

H: Enseñar a pronunciar y hablar

N: Números

PI: Pistas de interpretación para eliminar ambigüedades de la lectura labial

PR: Fomentar la práctica de la lectura labial.

C4. Actores del proceso de comunicación en la lectura labial

Establece quiénes pueden comunicarse al aprender la lectura labial.

SS: Entre sordos

SO: Sordos con oyentes

C5. Edad del grupo objetivo al que se dirige la enseñanza

Define el grupo etario al que se enfoca la herramienta utilizada en el proceso educativo.

N: niños en edad escolar (5 a 11 años)

A: Adolescentes (12 a 17 años)

AD: Adultos (18 años en adelante)

NE: No especificada

C6. Sistemas de comunicación utilizados

Identifica el sistema de comunicación que se aplica para el proceso de EA.

LS: Lengua de Señas

LE: Lengua escrita

LH: Lengua hablada

NE: No especificada

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

Los criterios C7 a C12 se orientan al enfoque tecnológico, contribuyen a identificar el tipo de desarrollo, la documentación de soporte, el tipo de tecnología y elementos de realidad extendida y/o multimedia que reportaron las aplicaciones analizadas, los métodos de acceso y modelo de negocios aplicados respectivamente. En la Tabla 4 se presentan los criterios mencionados.

TABLA IV. CATEGORÍAS DE CLASIFICACIÓN POR EL ENFOQUE TECNOLÓGICO

C7. Tipo de Software

Especifica el tipo de desarrollo de la aplicación.

L: Software de libre licenciamiento

P: Software propietario

C8. Documentación de soporte

Refiere si la aplicación posee documentación técnica o detallada de soporte.

T: Tesis doctoral

PI: Proyecto de investigación

PR: Prototipo

C9. Tecnología de uso

Indica el tipo de tecnología de acceso.

PC: Computador personal de escritorio

M: Móvil como tabletas o celulares

NE: No especificado

C10. Elementos de RE y/o multimedia utilizados

Define los elementos de RE (animaciones 3D y gafas de RA), así como los elementos multimedia (combinar texto, imágenes, audio, video), que utilizan los recursos tecnológicos analizados.

T: Texto

I: Imágenes o gráficos

S: Audio o sonido

V: Video

A: Animaciones 3D (avatares o cabezas parlantes)

GA: Gafas de RA

C11. Métodos de acceso a páginas web

Establece el tipo de acceso del usuario a la página web.

R: Registro

L: Libre o sin registro

C12. Modelos de negocios aplican las páginas web

Determina el modelo de negocio que la página web aplica.

P: Pago

G: Gratuito

IV. ANÁLISIS DE RESULTADOS

A. ENFOQUE ACADÉMICO Y TECNOLÓGICO DE LAS PUBLICACIONES ANALIZADAS

En cuanto al enfoque académico, las soluciones tecnológicas orientadas a enseñar la lectura labial se han apoyado en métodos académicos reproductivos que le permiten al instructor mediante una clase expositiva- demostrativa enseñar visemas, es decir la representación visual del sonido y la importancia de reducir errores de interpretación del discurso por lo que enfatizan en el proceso de enseñanza la similitud visual del sonido que presentan algunas consonantes.

De forma progresiva, los autores refieren la importancia de integrar al trabajo de interpretación del discurso a más del área de los labios, la cara y la parte superior del torso, de tal forma que, el lector visual puede ser capaz de interpretar e incorporar señales adicionales al mensaje que percibe. Inclusive mencionan aspectos relevantes que pueden interferir en el proceso de lectura tales como: a) la forma de los labios, b) articulación de las palabras, c) los acentos de las regiones de un país y/o de un idioma, d) nivel de iluminación, f) visibilidad de la boca, otros.

El proceso de enseñanza contempla la práctica y evaluación del estudiante para medir su progreso durante la adquisición del conocimiento, y las técnicas aplicadas para tales fines combinan: a) el uso de juegos serios, b) completar contenido de oraciones, c) historias narrativas, d) preguntas con respuestas múltiples, e) reproducir actividades como por ejemplo la vocalización de visemas y, f) el desarrollo de ejercicios, los que están inmersos en la misma aplicación permitiendo la práctica en línea o archivos que se pueden descargar e imprimir para realizarla posteriormente. Para ambos casos, la retroalimentación está presente de manera sincrónica o asincrónica.

Entre las principales habilidades que se busca desarrollar en las personas sordas está el garantizar que puedan desenvolverse y comunicarse en un entorno mixto (sordos y oyentes). Pero al existir posibles errores de interpretación en la lectura labial, es importante centrarse en el contexto y mantenerse informado de lo que sucede alrededor, de tal forma que la información previa que posee le permita ubicarse en la conversación. Por esta razón, se evidencia en las aplicaciones analizadas que el material de enseñanza-práctica se orienta: a) pronunciación y habla, b) enseñar vocabulario, c) reconocer palabras como unidades dentro del contexto y las oraciones.

Las soluciones tecnológicas que enseñan lectura labial se enfocan a satisfacer las diferentes tipologías: a) sordos congénitos, b) sordos con oído residual apoyados en el uso de implantes cocleares o audífonos y c) oyentes que por alguna enfermedad o accidente perdieron la audición, ya que permiten capacitar tanto a oyentes como sordos que deseen desarrollar esta habilidad siendo requisito previo saber leer y escribir para entender las indicaciones que cada una expone o ser asistido por un profesor/familiar para usarse como herramienta de apoyo al proceso de enseñanza-aprendizaje.

En relación con los sistemas de comunicación, las aplicaciones se apoyan en el uso de la lengua oral y/o escrita a manera de traducción en línea de la lectura labial que se enseña dejando en segundo plano el uso de la lengua de señas.

A manera de resumir la información obtenida de las publicaciones, se presenta en la Tabla 5 las publicaciones desde el enfoque académico.

Las publicaciones analizadas son el resultado de socializar investigaciones en diferentes etapas de desarrollo de proyectos y/o tesis doctorales, sin embargo, no siempre se encuentran disponibles los prototipos o documentación de soporte que permitan conocer con mayor detalle la investigación sin que sus repositorios de almacenamiento los hagan públicos o sean de libre acceso.

Las características de las TICs como la ubicuidad, la portabilidad y adaptabilidad permiten que las aplicaciones sean accesibles desde computadores de escritorios, portátiles (celulares, tablets, otros) o ambos, permitiendo el aprendizaje desde cualquier lugar y momento.

Finalmente, para potenciar el uso de la tecnología orientada a enseñar la lectura labial, se utilizan recursos tradicionales como el texto, la imagen, el audio y el video, estimulando y reforzando los procesos cognitivos que promuevan el aprendizaje.

Sin embargo, algunas aplicaciones integran tecnología de RE para potenciar progresivamente el proceso de enseñanza- aprendizaje dando lugar a tener profesores virtuales que asistan la enseñanza de manera autónoma o gafas de RA que den pistas de contextos de la interpretación de la lectura labial que interpreta el usuario. En la Tabla 6, se resumen las publicaciones desde el enfoque tecnológico.

TABLA VI. PUBLICACIONES CLASIFICADAS POR EL ENFOQUE TECNOLÓGICO SEGÚN: TIPO DE SOFTWARE (C7); DOCUMENTACIÓN AMPLIADA (C8); TECNOLOGÍA UTILIZADA (C9); ELEMENTOS DE RE UTILIZADOS (C10)

Ref.	*C7*	*C8*	*URL*	*C9*	*C10*
[25]	*P*	*T*	*1*	*PC*	*T, I, S, V*
[26]	*NE*	*NE*	*NE*	*PC*	*T, I, S, V*
[27]	*L*	*NE*	*NE*	*M*	*T, I, S, V*
[28]	*NE*	*NE*	*NE*	*PC*	*T, I, S, V, A (avatar 3D)*
[29]	*L*	*PI*	*2*	*PC, M*	*T, I, S, V, A (Cabeza parlante 3D)*
[30]	*L*	*PR*	*3*	*PC, M*	*NA*
[31]	*NE*	*NE*	*NE*	*NE*	*GA*

B. APLICACIONES MÓVILES PARA ANDROID

Las aplicaciones móviles analizadas utilizan una metodología reproductiva y se apoyan de forma integrada en videos, texto y audio cuando se enfoca a enseñanza mientras que si la orientación es un juego utiliza solo texto y audio por separados, donde este último aplica las características de distractor para el trabajo de interpretación que debe realizar [32], [33].

Estas soluciones tecnológicas están en idioma inglés, y aplican los modelos de negocios de pago y gratuitos, se dirigen a público oyente y sordos que deben como requerimientos mínimos saber leer y escribir para entender las instrucciones y participar del proceso de enseñanza o juego.

La Tabla 7 resume las aplicaciones móviles con Sistema Operativo Android analizadas, expone el nombre de la aplicación, su alcance, técnica aplicada, elementos de realidad extendida y sistemas de comunicación utilizados, así como el modelo de negocio que aplican.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

TABLA VII. CARACTERÍSTICAS DE LAS APLICACIONES ANDROID POR TÉCNICA APLICADA (C2), ELEMENTOS DE RE UTILIZADOS (C10), SISTEMA DE COMUNICACIÓN (C6), MODELO DE NEGOCIO (C12)

Aplicación	*Alcance de la página web*	*C2*	*C10*	*C6*	*C12*
Lips *Reading Academy (Dong Digital)*	*Enseña los sonidos del habla del Alfabeto Fonético Internacional agrupados por categorías, utiliza videos tutoriales (audio y texto). Versión gratuita: enseña consonantes y vocales, incluyen niveles con ejercicios prácticos presentados sin audio, son de opción de respuesta retroalimentación inmediata y puntaje obtenido. Se puede iniciar y alternar las clases según decida el usuario. Versión premium (suscripción lifetime $ 3,49 o mensual $ 1,07): incluye categorías de números, palabras y frases. Permite certificarse por categoría cursada cumpliendo la realización de todos los tutoriales y ejercicios con al menos el 50% del puntaje.*	*AV,* *P R*	*T,S, V*	*LE, LO*	*G, P*
Read my lips (Maxim Tros-chinsky)	*Juego de parejas. Al jugador 1 se le presentan varias palabras por 180 segundos que debe exponer sin audio a su compañero (cada 20 segundos esta cambia), el jugador 2 debe interpretarla y puede elegir la opción del juego de "escuchar música" que sirve como distractor y ayuda a respetar las normas del juego. No se permite hacer señas, gestos ni ningún otro medio de apoyo para dar a conocer la palabra.*	*RA*	*T*	*LE*	*G*

C. RECURSOS DISPONIBLES EN LAS PÁGINAS WEB

El potenciar las habilidades de comunicación de las personas sordas ha permitido la implementación de páginas web que aplican modalidades gratuitas, de pago o mixtas para acceder a aprender la lectura labial indistintamente si se es sordo u oyente, manteniendo la metodología reproductiva a través de la visualización de videos que exponen las formas de los visemas junto con las técnicas de resolución de ejercicios de interpretación con preguntas y alternativas de respuestas, reproducir actividades y/o el desarrollo de ejercicios, considerando como único requisito el saber leer y escribir para entender las indicaciones que presenta la página web [34].

El personalizar el ambiente y seguimiento de aprendizaje es una de las opciones que algunas de estas páginas adoptan al solicitar un registro de usuario antes de ingresar al entorno de aprendizaje en línea, que combina no de forma obligatoria el uso de audios en sus videos con la finalidad de transmitir el entorno natural del estudiante sordo al oyente mientras enseña el vocabulario y oraciones de uso cotidiano [35].

El internet tiene un alcance universal, y ha permitido encontrar páginas en diferentes idiomas como inglés, catalán y español, por lo que es importante recalcar que el usuario sordo debe optar por buscar páginas web creadas en el idioma de su país de origen, ya que la pronunciación de las palabras e inclusive los dialectos utilizados pueden confundirlo al desarrollar la habilidad de la lectura labial

Entornos web como Lectura labial, *Lipreading Practice, Lipreading y Read our Lips* refieren recomendaciones respecto a la adquisición de nuevos conocimientos tales como:

a) El tiempo de dedicación diario, b) repetir actividades prácticas en base al puntaje obtenido, c) retomar la práctica de lecciones anteriores luego de varios días para observar mejoras de puntuaciones o mayor seguridad en la resolución en los ejercicios, d) utilizar material complementario como medio de apoyo y práctica adicional, e) realizar descanso mental y visual luego de 15 o 20 minutos por el nivel de concentración y trabajo necesarios que demanda la lectura labial, f) recordar que no se utilizan nombres de letras sino el sonido que estas hacen, g) importante conocer el contexto y el análisis de las oraciones dentro de él combinados con análisis de gestos, expresiones faciales y corporales, g) aprender a identificar y observar los movimientos

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

importantes de la boca (labios, mandíbulas, dientes, lengua), h) comprender sus propios desafíos auditivos, tiempos de aprendizaje y necesidades de comunicación, así como el i) utilizar un bolígrafo y papel para escribir las palabras u oraciones que crea que ve mientras se mira el video.

Los recursos en línea al fomentar el auto aprendizaje suelen ofrecer material complementario de refuerzo para ser consultado de forma sincrónica o asincrónica tal como lo exponen las páginas de Lectura Labial, Escuela para sordos, Lipreading Practice, y Read our Lips en las que aplican técnicas de reproducción de actividades y desarrollo de ejercicios puntuales para reforzar el proceso de enseñanza-aprendizaje.

La Tabla 8 resume las características relevantes de las páginas web analizadas y se presenta al final del artículo.

D. PRINCIPALES HALLAZGOS DE LOS ENFOQUES ACADÉMICOS, TECNOLÓGICOS, Y DE LOS RECURSOS DISPONIBLES EN PÁGINAS WEB Y APLICACIONES MÓVILES

A manera de resumen, se presentan los principales hallazgos de los enfoques aplicados a las publicaciones y recursos analizados en este artículo, como metodologías educativas prevalece la reproductiva enfocada a un público lecto-escritor sordo/oyente a quienes se ofrece un sistema de enseñanza-aprendizaje independiente con opciones reducidas de interacción práctica entre pares y sin acompañamiento de tutores que los motiven y apoyen durante el proceso. Los ejercicios prácticos mayoritariamente son sincrónicos y el desarrollo del proceso educativo se apoya en audio, video, imágenes y textos, evidenciando la ausencia de uso de la lengua de señas.

Gran parte de los recursos (web y móviles) están disponibles para los usuarios mediante el uso de sus dispositivos móviles, sin exigir a cambio un registro ni restringirlos a través de métodos de pago, sin embargo, escasamente integran tecnología interactiva de RA, RV, o en general la RE. Respecto a las aplicaciones móviles, estas se presentan tanto como herramienta de enseñanza-aprendizaje y como juegos de aplicación práctica para grupos etarios de alrededor de 12 años en adelante.

En general, aquellas aplicaciones que surgen a partir de proyectos de investigación no ofrecen documentación técnica salvo pocas excepciones que se derivan de tesis académicas. Grupos de niños sordos en edad escolar no han sido prioritarios para el desarrollo de soluciones tecnológicas de enseñanza-aprendizaje relacionados con la lectura labial dejando de lado nuevos enfoques que pueden ser interesantes explorar a mediano y largo plazo.

V. DISCUSIÓN

La tecnología educativa para enseñar la lectura labial evidencia un gran desafío académico en el desarrollo de esta habilidad, ya que las soluciones tecnológicas podrían integrar técnicas y métodos activos-pasivos a más de las de tipo reproductivo que predominan en los hallazgos, buscando potenciar la enseñanza centrada en el estudiante motivándolo a investigar y aprender.

Al tener varias opciones educativas móviles, orientarse hacia un público lecto-escritor, y su contenido estar organizado de manera sugerente al proceso de enseñanza- aprendizaje que debería adoptarse, le dan la libertad al estudiante de experimentar y/o cambiar la tecnología por otra alternativa, en caso de que alguna de ellas, no llegue a cumplir con sus expectativas planteadas. Sin embargo, padres y tutores de niños sordos, que deben apoyar el proceso de aprendizaje de la lengua oral en edades tempranas, no disponen de soluciones de este tipo, inclusive cuando en el aula, ya se tienen niños que son nativos digitales.

Las aplicaciones analizadas a excepción de las móviles han explotado de manera básica los modelos lúdicos y de gamificación con orientación a un público joven-adulto mientras que, al potenciarlas se puede motivar e integrar un mayor número de personas, con diferentes rangos de edades e inclusive el proceso de aprendizaje pese a la carga metacognitiva que demanda puede resultar menos pesado para el estudiante.

Elementos tales como: las experiencias previas del interlocutor sordo respecto a una situación o entorno determinado, información actualizada del tema específico a tratarse y la amplitud de su vocabulario, confluyen positivamente al desarrollo del proceso de la lectura labial, permitiéndole entender el contexto de la conversación en la que participará, por tanto, el diseño de las aplicaciones debería contemplar el generar pautas que le ayuden a su pronta identificación complementándose con otras características que cubran sus necesidades especiales de usuario como por ejemplo, el uso de elementos multimedios, textos e imágenes, entre otros.

Se evidenció en las publicaciones el uso de gafas de RA como herramienta asistencial, más no aplicada como elemento de interacción en el proceso de enseñanza-aprendizaje o que promuevan actividades interactivas y/o colaborativas entre grupos tal como lo refieren algunas aplicaciones de aprendizaje de lengua de señas. Las bondades de un mundo conectado y ubicuo a partir del uso del internet y los dispositivos móviles podrían empoderar herramientas tecnológicas enfocadas a enseñar y desarrollar la habilidad de la lectura labial aprovechando recursos como la videocámara y el audio para combinarlos con los elementos de RA.

Como trabajos futuros se espera desarrollar una aplicación tecnológica que permita enseñar la lectura labial a los grupos excluidos conformados por niños en edad escolar, abriendo campo a nuevas líneas de investigación que permitan integrar metodologías activas centradas en el estudiante, buscando explorar técnicas educativas como la gamificación, colaboración, exploración, entre otras, desde los diferentes enfoques que plantea Kolb, promoviendo aprendizajes mediados que combinen tutorías escuela-casa, todo lo anterior apoyado en el uso de la tecnología móvil.

VI. CONCLUSIONES

El presente estudio evidencia la necesidad de diversificar el uso de la tecnología con medios audiovisuales para dotar de herramientas complementarias de comunicación a las personas sordas como, por ejemplo, enseñar la lectura labial a diferentes grupos etarios, apoyados en una combinación de métodos y técnicas educativas que promuevan mayor participación del estudiante entre pares o familiares oyentes, que ayuden a reforzar el proceso de enseñanza-aprendizaje y contribuyan a su inserción en entornos inclusivos [9], [36], [19].

Las soluciones educativas que se desarrollen a futuro, deben fortalecer la enseñanza y diversificación del vocabulario, así como su aplicación a los diferentes contextos cotidianos de una persona sorda, fomentando en ellos el estar informados sobre temas de actualidad de su entorno para que tengan mayor información que les permita definir el contexto de sus conversaciones [37], [38].

Las herramientas asistenciales aportan al cumplimiento de las diferentes actividades que una persona debe realizar de una manera más sencilla, más no libera la responsabilidad y el compromiso con la sociedad del enfoque y desarrollo de tecnología que fomenten el aprendizaje de temas específicos, potenciando principalmente para las personas sordas el uso de elementos audiovisuales pues el audio estimula el cerebro con la voz y las imágenes refuerzan los mensajes que deben ser capaces de interpretar en la lectura labial, considerando criterios de diseño y evaluación centrados en el usuario, procurando un equilibrio entre la carga visual y cognitiva que se integra [39], [40].

Las aplicaciones educativas analizadas, escasamente se apoyan en métodos lúdicos y colaborativos, mucho menos como videojuegos a fin de promover el proceso de aprendizaje desde un enfoque motivador y que integre la participación entre pares a partir del uso de dispositivos móviles [41], [42].

En general, se han definido nuevos enfoques académicos a partir de los cuales se puede afianzar la idea de desarrollar a futuro una herramienta educativa para enseñar la lectura labial a niños sordos en edad preescolar, combinando metodologías educativas mixtas aprovechando la tecnología móvil, otra opción a considerarse dentro de la misma línea podría ser el potenciar el uso de la realidad extendida, inicialmente la RA, fusionada con el uso de dispositivos móviles.

REFERENCIAS

[1] Caiza, Juan José; Villalba, Katerine Márceles; Chanchí, G. E. (2020). Herramienta tecnológica disruptiva para la inclusión social en personas sordas. Revista Ibérica de Sistemas e Tecnologias de Informação. https://www.proquest.com/docview/2385759327?pq-origsite=gscholar&fromopenview=true

[2] Comisión Económica para América Latina y el Caribe -CEPAL. (2011). Aprender y enseñar con las tecnologías de la información y las comunicaciones en América Latina: potenciales beneficios. In Publicaciones CEPAL. https://www.cepal.org/es/publicaciones/6177-aprender-ensenar-tecnologias-la-informacion-comunicaciones-america-latina

[3] Maas, M. J., & Hughes, J. M. (2020). Virtual, augmented and mixed reality in K–12 education: a review of the literature. Taylor & Francis Online, 29(2), 231–249. https://doi.org/10.1080/1475939X.2020.1737210

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

[4] Mann, S., Furness, T., Yuan, Y., Iorio, J., & Wang, Z. (2018). All Reality: Virtual, Augmented, Mixed (X), Mediated (X,Y), and Multimediated Reality. ArXivLabs. https://arxiv.org/abs/1804.08386v1

[5] Sánchez-García, J. M., & Toledo-Morales, P. (2017). Tecnologías convergentes para la enseñanza: Realidad Aumentada, BYOD, Flipped Classroom. Revista de Educación a Distancia (RED), 55(55), 22–34. https://revistas.um.es/red/article/view/315351

[6] Rosell Puig, W., & Paneque Ramos, E. R. (2009). Consideraciones generales de los metodos de enseñanza y su aplicacion en cada etapa del aprendizaje. Revista Habanera de Ciencias Médicas, 8(2). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1729-519X2009000200016

[7] Tecnologías de Inclusión CEDETi UC. (n.d.). Sueñaletras. CEDETi UC - Software Educativo. http://www.cedeti.cl/tecnologias- inclusivas/software-educativo/suenaletras/

[8] Tello, O., Varela, J., & Palos Toscano, Ú. (2018). Revisión teórica sobre los factores que influyen en el desarrollo de la competencia lectora de personas sordas. UARICHA, 14, 30–46. https://www.researchgate.net/publication/323128605_Revision_teorica_sobre_los_factores_que_influyen_en_el_desarrollo_de_la_competencia_lectora_de_personas_sordas

[9] Cruz Marte, C. E. (2017). ¿Qué opinan las personas sordas sobre el aprendizaje de la lengua escrita? Ciencia y Sociedad, 42(4), 73–82. https://doi.org/10.22206/cys.2017.v42i4.pp73-82

[10] Diario El Telégrafo. (2018). Con la lengua de señas, todos están incluidos. https://www.eltelegrafo.com.ec/noticias/sociedad/6/lengua- senas-inclusion

[11] Consejo Nacional de Igualdad de Discapacidades - (CONADIS). (2014). Diccionario Gabriel Roman. http://www.plataformaconadis.gob.ec/-platafor/diccionario/

[12] Bibish Kumar, K. T., John, S., Muraleedharan, K. M., & Sunil Kumar, R. K. (2021). Linguistically involved data-driven approach for Malayalam phoneme-to-viseme mapping. Applied Speech Processing, 117–145. https://doi.org/10.1016/B978-0-12-823898-1.00003-5

[13] Fonoaudiólogos. (2012). Aprendizaje de lectura labiofacial (LLF). https://fonoaudiologos.wordpress.com/tag/visema/

[14] Microsoft Docs - Azure Cognitive Services. (2021). Cómo obtener eventos de postura facial para la sincronización de labios - Azure Cognitive Services | Microsoft Docs. https://docs.microsoft.com/es- es/azure/cognitive-services/speech-service/how-to-speech-synthesis-viseme?pivots=programming-language-csharp

[15] García Vallejo Septién, M. (2020). Guía práctica de comunicación y entendimiento para personas con problemas de audición. Técnica Septién. YouTube Lectura Labiofacial - Técnica Septién; YouTube. https://www.youtube.com/watch?v=2qcdDLjn6F8

[16] Mireia. (2020). Lectura Labial Técnica Septién. Blog Como Me Oyes. https://comomeoyes.com/blog/lectura-labial-tecnica-septien/

[17] Velasco, C., & Pérez, I. (2009). Sistemas y recursos de apoyo a la comunicación y al lenguaje de los alumnos sordos. Revista Latinoamericana de Educación Inclusiva. https://sid.usal.es/idocs/f8/art11923/sistemas_y_recursos_de_apoyo.pdf

[18] Garrison, K. (2019). Theorizing lip reading as interface design. Communication Design Quarterly Review, 6(4), 24–34. https://doi.org/10.1145/3309589.3309592

[19] Velasco, C., & Pérez, I. (2009). Sistemas y recursos de apoyo a la comunicación y al lenguaje de los alumnos sordos. Revista Latinoamericana de Educación Inclusiva.

[20] Peluso, L. (2018). Los Sordos, sus lenguas y su textualidad diferida. Traslaciones: Revista Latinoamericana de Lectura y Escritura, 5(9), 40–61. https://dialnet.unirioja.es/servlet/articulo?codigo=6895487

[21] Del Pezo Izaguirre, E., Abásolo, M. J., & Collazos, C. A. (2019). Educational methodologies for deaf children supported by mobile technology and extended reality: a systematic analysis of literature. IEEE - RITA.

[22] Del Pezo Izaguirre, E., Abásolo, M. J., & Collazos, C. A. (2020). Uso de tecnologías móviles y realidad extendida para personas sordas: Una revisión sistemática de la literatura de acceso abierto. XV Conferencia Latinoamericana de Tecnologías de Aprendizaje.

[23] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. https://doi.org/10.5144/0256-4947.2017.79

[24] Mena Roa, M. (2021). Android y iOS dominan el mercado de los smartphones. Statista. https://es.statista.com/grafico/18920/cuota-de-mercado-mundial-de-smartphones-porsistema-operativo/

[25] Gamze, S., Dalkilic, G., Kut, A., Cebi, Y., & Serbetcioglu, B. (2007). Computer Aided Lip Reading Training Tool. Online Submission, 2–5

[26] Nittaya, W., Wetchasit, K., & Silanon, K. (2018). Thai Lip-Reading CAI for Hearing Impairment Student. 2018 Seventh ICT International Student Project Conference (ICT-ISPC), 1–4. https://doi.org/10.1109/ICT-ISPC.2018.8523956

[27] Gorman, B. M., & Flatla, D. R. (2018). MirrorMirror: A mobile application to improve speechreading acquisition. Conference on Human Factors in Computing Systems - Proceedings, 2018-April. https://doi.org/10.1145/3173574.3173600

[28] Gebert, H., & Bothe, H. H. (2010). LIPPS - a virtual teacher for speechreading based on a dialog-controlled talking-head. ICCHP'10: Proceedings of the 12th International Conference on Computers Helping People with Special Needs: Part I, 621–629. https://dl.acm.org/doi/abs/10.5555/1886667.1886781

[29] Czap, L. (2018). Online subjective assessment of the speech of deaf and hard of hearing children. Periodica Polytechnica Electrical Engineering and Computer Science, 62(4), 126–133. https://doi.org/10.3311/PPee.9215

[30] Muljono, M., Saraswati, G., Winarsih, N., Rokhman, N., Supriyanto, C., & Pujiono, P. (2019). Developing BacaBicara: An Indonesian Lipreading System as an Independent... International Journal of Emerging Technologies in Learning (IJET), 14(4), 44–57

[31] Gorman, B. M., & Flatla, D. R. (2017). A framework for speechreading acquisition tools. Conference on Human Factors in Computing Systems - Proceedings, 2017-May, 519–530. https://doi.org/10.1145/3025453.3025560

[32] Gil González, S. (2013). Cómo hacer Apps accesibles. Recuperado en mayo 14, 2022, de http://riberdis.cedid.es/handle/11181/4171

[33] UNESCO. (n.d.). Aprendizaje móvil. Las TIC En La Educación. Recuperado en mayo 14, 2022, de https://es.unesco.org/themes/tic- educacion/aprendizaje-movil

[34] González Fernández, A. (2017). El papel del diseño pedagógico en los entornos virtuales de educación digital. In Actas I Encuentro de doctorados e investigadores noveles. https://dialnet.unirioja.es/servlet/articulo?codigo=7718599

[35] Gonzalez, Marcela P. Benchoff, Delia Esther Huapaya, Constanza Raquel Remón, C. A., Lazurri, G., Guccione, L., & Lizarralde, F. Á. J. (2018). Avances en la personalización y adaptación de pruebas en un ambiente virtual de aprendizaje. http://sedici.unlp.edu.ar/handle/10915/73088

[36] Ministerio de Educación y Formación Profesional - Gobierno de España. (n.d.). Red Intergubernamental Iberoamericana de Cooperación para la Educación de Personas con Necesidades Educativas Especiales (RIINEE) - Ministerio de Educación y Formación Profesional. http://www.educacionyfp.gob.es/contenidos/ba/actividad- internacional/cooperacion-educativa/riinee.html#ancla0-6

[37] Herrera F, V. (2005). Habilidad linguistica y fracaso lector en estudiantes sordos. Estudios Pedagógicos (Valdivia), 31(2), 121–135. https://doi.org/10.4067/S0718-07052005000200008

[38] Holmer, E., Heimann, M., & Rudner, M. (2017). Computerized Sign Language-Based Literacy Training for Deaf and Hard-of-Hearing Children. The Journal of Deaf Studies and Deaf Education, 22(4), 404–421. https://doi.org/10.1093/deafed/enx023

[39] Sarmasik, G., Dalkilic, G., Kut, A., Cebi, Y., & Serbetcioglu, B. (2007). Computer Aided Lip Reading Training Tool. In Online Submission.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

[40] Sierra-Martínez, L. M., Golondrino, P. G. E. C., & Álvarez, P. M. C. G. (2022). Directrices para el diseño y la construcción de videojuegos serios educativos. Revista Colombiana de Educación, 1(84). https://doi.org/10.17227/rce.num84-12759

[41] Cruz-Lara, S., Fernández Manjón, B., & Vaz de Carvalho, C. (2013). Enfoques Innovadores en Juegos Serios. Enfoques Innovadores En Juegos Serios. IEEE VAEP RITA, 1(1), 19–21. http://seriousgamesnet.eu/community

[42] Taipe, M. A., Taipe, M. S. A., Pesántez, D. Á., Rivera, L., & Vizueta, D. O. (2017). Juegos Serios en el Proceso de Aprendizaje. UTCiencia "Ciencia y Tecnología Al Servicio Del Pueblo," 4(2), 111–122. http://investigacion.utc.edu.ec/revistasutc/index.php/utciencia/article/ view/70

TABLA V. PUBLICACIONES CLASIFICADAS POR EL ENFOQUE ACADÉMICO SEGÚN: MÉTODO ENSEÑANZA-APRENDIZAJE (C1); TÉCNICA APLICADA (C2); ÁREA DE ENSEÑANZA (C3); USUARIOS (C4); EDAD USUARIOS (C5); SISTEMA DE COMUNICACIÓN (C6)

Ref.	Alcance	C1	C2	C3	C4	C5	C6
[25]	AURIS, ayuda a profesores en su práctica de enseñar la lectura labial tal como se usa en conversaciones cotidianas. Requiere ingresar la edad del usuario y nivel de aprendizaje. Permite elegir entre las opciones de aprendizaje: quién soy yo, juguetes, mi familia. Al seleccionar una palabra se muestra un video de la pronunciación de la palabra y otro en donde se usa el objeto. Se puede personalizar con imágenes del niño y su familia, el niño puede grabar su pronunciación y compararla visualmente con la del instructor	R	AV, AC	P	SS	N	LE, LH
[26]	Aplicación que enseña vocabulario, los estudiantes verán un video del movimiento de la boca que pueden practicar fruta, animal, equipo, vegetal y vehículo, cada una tiene 20 palabras que tienen una o tres sílabas. Hay veinte preguntas por ronda. El usuario puede buscar una palabra específica.	R	G, AV, PR	V	SS,SO	N	LS, LE, LH
[27]	"Mirror Mirror", aplicación Android que permite practicar la lectura de discursos grabando y viendo videos de sus videos en bibliotecas, etiquetarlos y agruparlos por su forma de los labios, palabras y hablantes; activar/desactivar los audios según requiera. Se puede configurar a otros idiomas además del inglés.	R	FE, AV, RA, DE	PR	SS,SO	A	LE, LH
[28]	Crean un profesor virtual con una cabeza parlante que puede tener un diálogo abierto (sobre situaciones cotidianas) o guiado (basado en preguntas y respuestas). Puede cambiar su apariencia y voz, maneja animación facial sincronizando la síntesis de la voz. El módulo de profesor permite crear y personalizar cada tipo de diálogo con unidades de contenido con distractores visuales/ auditivos (girar la cabeza del avatar, colocar +/- luz, imágenes de fondo, ruido, otros). El módulo del estudiante permite elegir con qué desea trabajar: lección (diálogo libre) o guiado	R	AV, PR	N	SS	NE	LE, LH
[29]	[29] Speech Assistant cabeza parlante 3D que enseña a los niños sordos a hablar o mejorar la producción del habla mediante la visualización del discurso hablado y su articulación. Permite escuchar y ver la palabra (los ángulos de inclinación de la lengua para una mejor retroalimentación de lo enseñado). Graba su aprendizaje, compara resultados a través de la práctica que el sistema evalúa automáticamente. El profesor puede dar seguimiento al proceso evolutivo del estudiante y añadir comentarios. Puede ser adaptado a más idiomas del húngaro.	R	AV, RA	H	SS,SO	N	LE, LH
[30]	[30] BacaBicara, sistema de e-learning con 11 lecciones que clasifican las vocales y consonantes por tipos, presenta ejercicios de práctica con cuestionarios interactivos de respuestas múltiples divididos en 15 temas con niveles fácil/medio/difícil. Permite hacer un seguimiento de los estudiantes, presenta estadísticas de su progreso, y proporciona apoyo de un instructor si alguien lo requiere. La aplicación envía recordatorios de los horarios de práctica/clases al teléfono móvil.	R	G, AV, PR,RA	P	SS,SO	NE	LE, LH
[31]	[31] Herramienta que permite visualizar una cantidad media de información analítica para mejorar su lectura labial en tareas de reconocimiento de palabras. Presentan 3 prototipos: a) MirrorTrainer ya desarrollada como MirrorMirror [26], b) PhonemeViz que coloca los caracteres del fonema inicial hablado más reciente justo al lado de los labios del hablante para ayudar a desambiguar los visemas confusos (superpuesto en video o mostrado en la cabeza del hablante), y c) ContextCueView mostrando señales de conversación (ideas generales en forma textual del contexto de la conversación) que se presentan a un lado del rostro del hablante.	NA	CC	PI	SS,SO	NE	LE

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

TABLA VIII. CARACTERÍSTICAS DE LAS PÁGINAS WEB SEGÚN: ELEMENTOS DE RE UTILIZADOS (C10), SISTEMA DE COMUNICACIÓN (C6), TIPO DE ACCESO (C11), MODELO DE NEGOCIO (C12), IDIOMA DE LOS RECURSOS, PAÍS

Dirección	Alcance de la página web	C10	C6	C11	C12	Idioma	País
http://ecturalabial.org/	23 lecciones en video incluyen la explicación y los ejercicios. 1 lección en inglés (enseña números y colores). Los ejercicios están en modo texto y se apoyan en el video: presentan opciones de respuesta múltiple, verdadero o falso, completar o elegir la respuesta que debe escribirse. Se puede dejar ejercicios sin responder y continuar con el desarrollo del siguiente. Los videos se presentan en un orden lógico y alfabético, el contenido se ha organizado por categorías tales como: actividades y fiestas, alimentos y bebidas, animales y plantas, colores formas y medidas, entre otras. Permite descargar el sitio web completo para trabajar las lecciones sin conexión a internet (descargado y funciona). Material complementario: Fichas de palabras clave y transcripción en formato PDF, 8 barajas compuestas por cartas con la configuración orofacial de los diferentes fonemas trabajados.	T, S, V	LE,LH	L	G	Gallego, castellano, inglés	España
https://www.escuelap arasordos.com/lectura-de- labios.php	Conjunto de actividades de 3 libros categorizados como 1 de oraciones simples y 2 de oraciones compuestas. Organiza las actividades prácticas por números, colores tipos de oraciones: atributivas, intransitivas. impersonales, otras. Las actividades no permiten dejar respuestas en blanco e incluyen ejercicios de: enlaces de preguntas y respuestas mediante técnica de arrastre con el ratón, escribir palabras u oraciones interpretadas con LB, seleccionar respuestas de un grupo de alternativas. Al final permite revisar los aciertos/desaciertos. Material complementario: Serie de tres libros impresos, se presenta las estructuras sintácticas de la lengua española; divididos en Estructuras Simples (libro 1), Estructuras Compuestas 1 (libro 2) y Estructuras Compuestas 2 (Libro 3), usando como base el Método Global de Análisis Estructural.	T, S, V	LE,LH	L	G	Español	México
http://yoleotuvideo.cl/basico/	Presenta los fonemas para entender cómo reconocerlos en las palabras. El contenido está agrupado por niveles: básico, intermedio, avanzado y experto; en los que se encuentran fonemas y temáticas (colores, frutas, verduras, saludos, profesionales, animales, otras). Los ejercicios incluyen: selección de la respuesta correcta desde un listado de palabras, adivinar la palabra faltante que se lee o dicta la profesora, responder las preguntas relacionadas con una historia corta. Permite monitorear el rendimiento por ejercicios realizados, tiempo de desarrollo y puntaje obtenido y promedio.	T, V	LE	R	G	Español	Chile

http://lipreadingpractice.co.uk/	*Página de práctica, presentan videos con tomas frontales y de perfil para la interpretación de la lectura de labios. Agrupan videos por categorías: consonantes, vocales, historias cortas/pasajes, frases diarias, números, ritmo/entonación, juego de memoria. Permite activar/desactivar subtítulos y volumen a preferencia del usuario. Material complementario: PDFs con lista de palabras para practicar con un amigo o frente a un espejo, enlazar palabras que se verán similares, frases para completar de manera escrita y para practicar frente al espejo (entender la frase), otras.*	*T, S, V*	*LE,LH*	*L*	*G*	*Inglés*	*Reino Unido*
https://www.lipreading.org/	*Capacitación de pago y tiene recursos gratuitos en el apartado de lecciones, tales como: a) juego en parejas de práctica de lectura de labios en vivo, se debe grabar una oración que la página provee, y la contraparte interpretar la palabra faltante, b) alfabeto de lectura de labios con videos, c) juegos con ejercicios de lectura de labios nivel básico y avanzado. El material se orienta a trabajar palabras y frases de uso diario.*	*T,V*	*LE*	*L,R*	*G,P*	*Inglés*	*EEUU*
http://www.read-my-ips.org.uk/	*Enseñan los visemas de las consonantes, historias cortas y ejercicios (el contenido de los videos no refiere frases o palabras de uso cotidiano). El video presenta la pronunciación con/sin audio y subtítulos con la finalidad de fomentar la práctica. Los ejercicios no son interactivos, el hablante menciona la frase con audio y título 2 veces, luego la repite para que el estudiante las identifique.*	*T,S,V*	*LE,LH*	*L*	*G*	*Inglés*	*Reino Unido*
https://www.readourlips.ca/	*Grupo de 8 lecciones que ofrecen certificación al final del curso. Enseñan los visemas de las consonantes, palabras y frases de uso cotidianos. Cada video está disponible desde un ángulo frontal y un ángulo lateral, solo los videos de la lección están con audio y subtitulado, los de práctica no. La velocidad de los videoclips se puede aumentar o disminuir. Cada lección se estructura: práctica de calentamiento con 5 ejercicios, 1 lección de enseñanza, práctica de palabras y de oraciones (cada una con 1 introducción y 5 ejercicios), repaso de la lección y recursos para la pérdida auditiva (diferentes lecturas en PDFs por cada lección). Los ejercicios están organizados y programados secuencialmente hasta dar con la respuesta correcta (5 a 7 palabras de práctica), se proporcionan opciones de respuesta. Si se obtiene una nota mayor al 80% se podrá pasar a la siguiente lección. Material complementario: Disponible en la lección # 1: a) ¿Qué es la lectura de discursos?, b) consejos para mejorar la comunicación, c) el triángulo de la comunicación.*	*T,S,V*	*LE,LH*	*R*	*G,P*	*Inglés*	*Canadá*

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

AUTHORS

Evelyn Del Pezo Izaguirre

Profesora de la carrera de Sistemas de Información, de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil (UG), en Guayaquil-Ecuador.
Máster en Sistemas de Información Gerencial graduada en la Escuela Superior Politécnica del Litoral (ESPOL). Ha impartido cursos de pregrado en la línea de Programación, Procesos, Comercio Electrónico y TICs. Trabajó en proyectos de vinculación con la comunidad en el Programa para el Desarrollo de la Península de Santa Elena (ESPOL), en proyectos educativos en la Universidad Santa María campus Guayaquil (USM).
Actualmente, es estudiante de doctorado en la Facultad de Informática de la Universidad Nacional de La Plata. Su investigación se orienta al área de Tecnología Informática en Educación con aplicación de las tecnologías a personas con necesidades especiales (niños sordos).
Áreas de Interés: educación, tecnología móvil, redes sociales, gobierno electrónico.

María J. Abásolo

Investigador de la Comisión de Investigaciones de la Provincia de Buenos Aires (CICPBA), profesor Asociado y miembro del III-LIDI de la Facultad de Informática de la Universidad Nacional de La Plata. Doctora en Informática por la Universidad de las Islas Baleares.
Áreas de Interés: Realidad Aumentada, Realidad Virtual.
Entre sus antecedentes de investigación actuales se mencionan:
- Miembro del proyecto acreditado UNLP Programa de Incentivos "Computación de Alto Desempeño: Arquitecturas, Algoritmos, Métricas de rendimiento y Aplicaciones en HPC, Big Data, Robótica, Señales y Tiempo Real" (2018-2021) dirigido por M. Naiouf.
- Miembro del proyecto acreditado UNLP Programa de Incentivos "Metodologías, técnicas y herramientas de Ingeniería de Software en escenarios híbridos. Mejora de proceso" (2018-2021) dirigido por P. Pesado
Ha impartido hasta la actualidad cursos de posgrado, en el Doctorado en Ciencias de la Facultad de Informática de la UNLP y en el Doctorado de Informática de la UIB, de las siguientes temáticas: Realidad Aumentada, Interfaces Avanzadas, Visualización 3D en Internet: VRML y X3D, Humanoides Virtuales, Visión estereoscópica, Reconstrucción 3D a partir de fotografías, Realidad Virtual, Métodos avanzados de informática gráfica: modelado de escenas 3D y Escenarios Virtuales e Interactivos.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763111

César A. Collazos

Profesor Titular del Departamento de Sistemas, de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca-Colombia, coordinador del grupo IDIS (Investigación y Desarrollo en Ingeniería del Software), coordinador de la Red HCI-Collab: Red Iberoamericana de apoyo a los procesos de enseñanza-aprendizaje de Interacción Humano Computador en países Iberoamericanos. Doctor en Ciencias mención Computación de la Universidad de Chile, con estancias postdoctorales en Chile y España. Ha dirigido diversas tesis doctorales en el uso de TIC para apoyar procesos de enseñanza aprendizaje, siendo unas de las últimas las realizadas para apoyar procesos de lecto-escritura en niños sordos.
Actualmente es el Presidente de la Sociedad Colombiana de Computación, y profesor de la Maestría en Computación y en el doctorado en Ciencias de la Electrónica de la Universidad del Cauca-Colombia. Ha dirigido más de 16 tesis doctorales, autor de diversos trabajos científicos en eventos y revistas reconocidas en los temas de Interacción Humano-Computador, Aprendizaje Colaborativo Apoyado por Computador.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol IX, Issue 2, July 2022

Desarrollo de una Aplicación Móvil para Manejar una Agenda Personal de Personas con Discapacidad Visual Total

Development of a Mobile Application to Manage the Personal Agenda of People with Total Visual Impairment

ARTICLE HISTORY

Received 25 March 2022
Accepted 2 May 2022

Jaime Crespin
Facultad de Ingeniería de Sistemas
Escuela Politécnica Nacional
Quito, Ecuador
jaime.crespin@epn.edu.ec

María Hallo
Facultad de Ingeniería de Sistemas
Escuela Politécnica Nacional
Quito, Ecuador
maría.hallo@epn.edu.ec

Desarrollo de una Aplicación Móvil para Manejar una Agenda Personal de Personas con Discapacidad Visual Total

Development of a Mobile Application to Manage the Personal Agenda of People with Total Visual Impairment

Jaime Crespin
Facultad de Ingeniería de Sistemas
Escuela Politécnica Nacional
Quito – Ecuador
jaime.crespin@epn.edu.ec

María Hallo
Facultad de Ingeniería de Sistemas
Escuela Politécnica Nacional
Quito – Ecuador
maria.hallo@epn.edu.ec

Resumen— En el presente trabajo se desarrolla una aplicación móvil de agenda personal orientada a personas con discapacidad visual total, que funcione a manera de agenda personal apoyando a la falta de esta funcionalidad en aplicaciones existentes. La aplicación permite agregar contactos, listar eventos agendados, programar recordatorios personalizados y notificar eventos a los contactos. El proyecto fue desarrollado utilizando una metodología de diseño de la investigación y el marco de trabajo Scrum para el desarrollo del artefacto, Scrum permite que exista una mejor planificación de las tareas dentro del desarrollo de la aplicación móvil. Además, facilita los cambios o nuevos requisitos que surgieron durante el desarrollo de la aplicación móvil. El proyecto se lo dividió en un total de 6 Sprints de aproximadamente 2 semanas cada uno. La aplicación móvil fue desarrollada utilizando el lenguaje de programación Kotlin, y se realizó una integración con la base de datos Firebase RealTime Database para el almacenamiento de una encuesta de usabilidad integrada dentro de la aplicación. Para el desarrollo de las pruebas de accesibilidad y usabilidad se contó con el apoyo de la Fundación PROCODIS (Promotora de Comunicadores con Discapacidad Visual), personas con discapacidad visual que poseen experiencia utilizando dispositivos móviles. Además, las pruebas de accesibilidad se las realizó utilizando herramientas propias de Google para dispositivos Android a lo largo del desarrollo de la aplicación.

Palabras claves— *discapacidad visual, accesibilidad, scrum, aplicación móvil*

Abstract— In this work, we develop a personal agenda mobile application oriented to people with total visual impairment, which works as a personal agenda supporting the lack of this functionality in existing applications. The application allows adding contacts, listing scheduled events, scheduling personalized reminders and notifying events to contacts. The project was developed using a research design methodology and the Scrum framework for the development of the artifact, Scrum allows for better planning of tasks within the development of the mobile application. In addition, it facilitates changes or new requirements that arose during the development of the mobile application. The project was divided into a total of 6 Sprints of approximately 2 weeks each. The mobile application was developed using the Kotlin programming language, and an integration with the Firebase RealTime Database was performed for the storage of a usability survey integrated within the application. For the development of the accessibility and usability tests we had the support of the PROCODIS Foundation (Promotora de Comunicadores con Discapacidad Visual), people with visual impairment who have experience using mobile devices. In addition, accessibility tests were performed using Google own tools for Android devices throughout the development of the application.

Keywords— *visual disability, accessibility, scrum, mobile application*

I. INTRODUCCIÓN

En la actualidad, la tecnología móvil se ha extendido rápidamente y es indiscutible que su uso para realizar tareas y/o actividades cotidianas es mucho más común de lo que era anteriormente. Los móviles ya no son utilizados únicamente para realizar llamadas y enviar mensajes, sino que gracias a las tecnologías actuales permiten realizar actividades cada vez más complejas. La mayoría de las aplicaciones desarrolladas para dispositivos móviles están pensadas con el objetivo de ofrecer facilidades y una grata experiencia de usuario, pero por lo general, su diseño está enfocado para ser utilizado por personas que no poseen

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

ningún tipo de discapacidad, pero como ya se pudo constatar, independientemente de las características físicas que posea una persona la necesidad de dar uso a las tecnologías actuales para realizar sus actividades diarias persiste, ya sea que puedan depender de aplicaciones y servicios para comunicarse, aprender e inclusive trabajar.

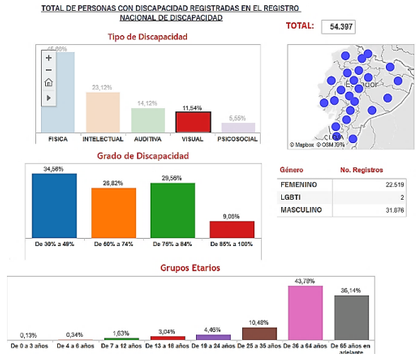


Fig.1 Estadísticas del 2022 de personas con discapacidad visual

La Figura 1 presenta los datos del Ecuador publicados por el Consejo Nacional para la Igualdad de Discapacidades (CONADIS) [1]. Existen 471.205 personas registradas con algún tipo de discapacidad, estas discapacidades se dividen en física, intelectual, psicosocial y visual. De este grupo, existen 54.397 personas con discapacidad visual registradas; población que corresponde al 11,54% de los ecuatorianos con alguna discapacidad. Para las personas con algún tipo de discapacidad, el uso de la tecnología no debería considerarse como un problema, sino más bien como una solución, ya que la tecnología usada de forma correcta tiene el potencial de reducir muchas de las barreras que impiden a las personas con algún tipo de discapacidad, participar en actividades cotidianas. Recientemente, en Ecuador se han desarrollado dos aplicaciones que han tenido un impacto positivo en las personas con discapacidad visual, estas aplicaciones son SpeakLiz-Vision y Hand Eyes. Ambas aplicaciones tienen como objetivo el facilitar la movilidad de las personas no videntes a través del uso de la tecnología [2].

El documento está estructurado en secciones. En la sección 2, se describe los trabajos relacionados con el contenido de este proyecto, en la sección 3 se encuentran los fundamentos teóricos sobre los que sustenta este trabajo. La sección 4 presenta la metodología utilizada para el diseño de la investigación. En la sección 5, se tiene el desarrollo de la aplicación. La sección 6 presenta el resultado obtenido mediante las pruebas de usabilidad de la aplicación. La sección 7 presenta las conclusiones, la sección 8 contiene información sobre los trabajos futuros y finalmente, en la sección 9 se tiene un agradecimiento.

II. TRABAJOS RELACIONADOS

En esta sección se describen trabajos relacionados con aplicaciones móviles enfocadas a personas con discapacidad visual, aplicaciones que ofrecen algún beneficio o mejora en las actividades que pueden realizarse dando uso de la tecnología, especialmente dispositivos móviles.

Actualmente, existen ciertas aplicaciones móviles destinadas a personas con algún tipo de discapacidad. Realmente estas aplicaciones se encuentran enfocadas a temas de movilidad, geolocalización y reconocimiento de objetos o imágenes. Existen estas aplicaciones porque estos temas son un mal común que las personas con discapacidad visual comparten. Para diseñar aplicaciones de este tipo se debe considerar que el desarrollo suele exigir ciertas características concretas, donde es necesario utilizar estándares que permitan validar su usabilidad y accesibilidad.

Además, estas aplicaciones no son diseñadas de la manera habitual, sino más bien cuentan con funcionalidades específicas, es distinto desarrollar una aplicación móvil enfocada totalmente para personas con discapacidad, que el tener una aplicación ya desarrollada y adaptarla para que pueda ser utilizada por personas con discapacidad. Entre los trabajos relacionados a temas de discapacidad podemos encontrar tres aplicaciones destinadas a personas con discapacidad visual, FarmaceuticApp, VOZ – TOUCH GPS y TransmiGuia [3][4].

TransmiGuia es una aplicación desarrollada en Colombia que permite a las personas utilizar el sistema de transporte público de manera más cómoda. Posee las siguientes características:

- Posee un menú práctico y sencillo, con un mensaje de bienvenida.
- Cuenta con reconocimiento de voz en la mayoría de sus pantallas.Informa al usuario de su ubicación actual.
- Genera una ruta hacia las paradas de transporte público con sus respectivas indicaciones.

VOZ – TOUCH GPS es una aplicación que posee funciones muy similares, fue desarrollada en Ecuador y permite al usuario conocer su

ubicación actual, la parada de transporte público más cercana, conocer las distintas rutas de los buses, realizar llamadas y enviar mensajes predeterminados de su ubicación.

Estas características se las puede observar a continuación:

- Posee una interfaz amigable y fácil manejo
- Hace uso de un sintetizador mediante el cual se genera texto a través de voz y viceversa.
- Posee retroalimentación auditiva en sus pantallas.
- Permite conocer información de ubicación y la parada de transporte público más cercana.

Por otra parte, FarmaceuticApp es una aplicación móvil la cual fue desarrollada en Colombia. Esta aplicación ofrece información sobre medicamentos, posee distintas formas para realizar búsquedas ya sea utilizando voz, texto o código de barras. Sus características se las puede observar a continuación:

- Tiene una interfaz sencilla.
- Hace uso de la cámara para poder buscar el medicamento por reconocimiento de imagen o mediante el código de barras.
- Posee retroalimentación auditiva en sus pantallas.
- Permite buscar medicamentos mediante comando de voz o realizar una búsqueda con texto.

Finalmente, en la tienda de Google Play para dispositivos móviles existen varias aplicaciones para el manejo de agenda o tareas diarias, aplicaciones como: TickTick, Any.do, Google Keep y el propio Google Calendar [5]. Sin embargo, algunas de ellas (TickTick y Any.do) solicitan iniciar de sesión para poder utilizarlas lo cual resulta en un mayor esfuerzo para poder empezar a usarlas, más aún si se tiene activado Google Talkback. Por otro lado, estas aplicaciones no permiten notificar de los eventos a un contacto en específico ni tampoco proveen del clima al momento de mostrar el recordatorio del evento. Estos últimos puntos, acompañados del hecho que AgendaVIP está pensada específicamente para personas con discapacidad visual, son las características de que la diferencian positivamente de las demás. A continuación, en la Tabla I se presenta un resumen comparativo de lo comentado anteriormente.

III. MARCO TEÓRICO

Una aplicación móvil se define en [6], como: "software autónomo diseñado para un dispositivo móvil y que realiza tareas específicas para usuarios móviles". Las aplicaciones móviles por lo general proporcionan a los usuarios servicios similares a los que se tienen desde las computadoras, estas aplicaciones son pequeñas unidades de software que poseen funciones limitadas, que sin embargo logran brindar a los usuarios servicios y funcionalidades que reflejan una experiencia de alta calidad.

TABLA I. Comparativa versus aplicaciones actuales

Aplicaciones / Características	Agenda VIP	Tick Tick	Any.do	Google Keep	Google Calendar
Funcionalidad por voz	X			X	
Agregar eventos		X	X		X
Agregar contactos	X				
Mostrar Eventos	X	X			X
Notificar evento a un contacto	X				
Enviar ubicación actual a un contacto	X				
Integración con Calendario de Google	X	X	X	X	X
Iniciar sesión		X	X		
Desarrollada para ser utilizada por persona con discapacidad visual mediante Google Talkback	X				

A. DISCAPACIDAD VISUAL

La discapacidad visual se define como una disminución de la capacidad de ver en tal grado que logran causar problemas, lo cuales no pueden ser solucionados utilizando medios convencionales, es decir, utilizando anteojos o medicamentos. La discapacidad visual puede ser causada por algún tipo de enfermedad, un traumatismo o afecciones congénitas – degenerativas [7].

B. ACCESIBILIDAD EN EL SOFTWARE

Se puede encontrar muchas definiciones de accesibilidad y varias de ellas se encuentran relacionadas con la palabra usabilidad. La guía ISO/IEC 71 [8] define el diseño basado en la accesibilidad como "diseño centrado en principios que extienden el diseño estándar u original hacia personas con algún tipo de limitación, con la finalidad de maximizar el número de usuarios que pueden utilizar fácilmente un producto, edificio o servicio". Por otro lado, en [9] definen a la accesibilidad como "usabilidad de un producto, servicio, entorno o instalación por personas con la más amplia gama de capacidades", introduciendo una estrecha conexión con la usabilidad. La accesibilidad dentro del ámbito informático [10] se define como la posibilidad de que un producto o servicio pueda ser accedido y utilizado por el mayor número de personas posibles, indiferentemente de las limitaciones propias del individuo. Como se puede observar, además de la accesibilidad es necesario también considerar los diseños basados en la usabilidad, donde se pretende la inclusión de personas que poseen algún tipo de discapacidad, para este proyecto en específico personas con discapacidad visual.

C. GOOGLE TALKBACK

Google Talkback es el lector de pantalla de Google que proporciona comentarios hablados sobre lo que se toca, selecciona o activa dentro de la pantalla, para que se pueda usar o controlar las acciones del dispositivo sin necesidad mirarlo. Este lector de pantalla se encuentra integrado por defecto en los dispositivos Android [11], la configuración varía según el fabricante, versión de Android y la versión mismo de Talkback.

D. FIREBASE

Firebase es considerada una plataforma de aplicaciones web que permite a los desarrolladores crear aplicaciones de alta calidad. Almacena los datos en formato de notación de objetos Javascript (JSON) el cual no utiliza consultas para insertar, actualizar o eliminar registros [12]. Firebase maneja la mayor parte del trabajo del lado del servidor, se utiliza como una base de datos de tiempo real en el desarrollo de aplicaciones tanto web como móviles.

E. WCAG 2.1

Las Pautas de Accesibilidad del Contenido Web 2.1 o WCAG 2.1 por sus siglas en inglés. Son una extensión de WCAG 2.0, donde se añaden criterios enfocados a la accesibilidad móvil, personas con baja visión y personas con discapacidad cognitiva y de aprendizaje [13].

Las pautas de accesibilidad se encuentran en 4 secciones principales, las cuales se muestran a continuación:

- *Perceptible:* La información y los elementos de la interfaz de usuario deben poder presentarse a los usuarios de forma que estos puedan percibirlos.
- *Operable:* Los elementos de la interfaz de usuario y la navegación misma, deben estar operables.
- *Comprensible:* La información y el funcionamiento de la interfaz de usuario deben ser comprensibles.
- *Robusto:* El contenido debe ser robusto para que pueda ser interpretado por la mayor cantidad de usuarios, incluidas las tecnologías de asistencia.

En la Tabla II se puede observar cuáles fueron las pautas consideras en el desarrollo y diseño del presente proyecto

TABLA II. Pautas De La WCAG 2.1 Considera

Sección	Pauta	Criterios
Perceptible	Texto alternativo	Contenido sin texto
	Adaptable	Secuencia significativa
		Orientación
	Distinguible	Proporción de contraste mínimo
		Uso del color
Operable	Navegación	Orden de enfoque
		Páginas tituladas
Comprensible	Asistencia en ingreso de datos	Identificación de errores
		Etiquetas o instrucciones
Robusto	Compatible	Compatibilidad con sistemas actuales y antiguos
		Compatibilidad con lectores de pantalla

IV. METODOLOGÍA

En este estudio se utilizó una adaptación de la metodología de diseño de investigación (design research methodology) que tiene las siguientes etapas:

- *Identificacion de la problemática:* El

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

problema puede identificarse identificarse a partir nuevos desarrollos o utilizando tecnologías actuales que permitan llegar al mismo resultado.

- *Sugerencia de solución:* Se logra diseñar y plantear la solución, la cual resultaría en un artefacto o producto final.
- *Desarrollo e Implementación:* Se realiza el desarrollo utilizando las técnicas que se necesiten dependiendo del producto que se busca obtener.
- *Discusión y Resultados:* Una vez terminado el desarrollo del artefacto, este se lo evalúa dependiendo del caso y se pone a prueba su aporte a la solución de la problemática.
- *Conclusiones y Trabajos Futuros:* En esta fase se concluye en lo que aporta el producto final con base a lo encontrado en la anterior fase.

V. DESARROLLO

Aplicando la metodología, se obtuvieron las siguientes etapas:

A. IDENTIFICACIÓN DE LA PROBLEMÁTICA

Para este trabajo, se ha identificado que el principal problema es la falta de aplicaciones móviles que cumplan la tarea de una agenda personal y que esté enfocado a personas con discapacidad visual.

B. SUGERENCIA DE SOLUCIÓN

Mediante la identificación de la problemática se plantea una solución ya sea utilizando componentes existentes o nuevos, debido al gran aumento en el uso de dispositivos móviles se sugiere una solución de tipo aplicación móvil enfocado a personas con discapacidad visual, el cual recibe el nombre de AgendaVIP (Agenda for Visual Impairment People)

C. DESARROLLO E IMPLEMENTACIÓN

Para el desarrollo del artefacto, una aplicación móvil, se utilizó el marco de trabajo Scrum que facilita la constante comunicación con las personas interesadas, en este caso personas con discapacidad visual. Entre las ventajas del uso del marco de trabajo Scrum se pueden mencionar: transparencia, mejora continua y adaptabilidad [14]. Adaptarse a los cambios durante el desarrollo, ya sea en etapas tempranas o finales, es primordial y más aún si se busca que una aplicación móvil sea accesible ya que es necesario que cuente con unas características concretas y que satisfaga ciertas directrices, las cuales pueden ir cambiando durante el desarrollo con base en las necesidades del usuario. Utilizando Scrum se puede llegar a reducir la dificultad y complejidad que conlleva el solventar problemas de accesibilidad, ya que mediante el proceso de entregas continuas se logra encontrar las deficiencias en etapas tempranas y pueden ser corregidas durante el desarrollo [15]. Además, Scrum es de mucha utilidad en el tema de comunicación continua con el usuario, el cual es un punto importante para lograr entregar un producto de calidad.

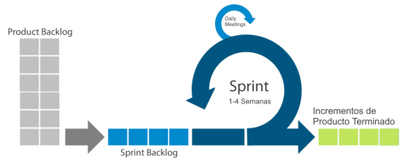


Fig2. Marco de trabajo Scrum

D. DEFINICIÓN DE REQUERIMIENTOS

La recopilación de requerimientos fue un proceso donde se realizó un análisis de las necesidades que poseen las personas con discapacidad visual en el manejo de actividades o eventos mediante su dispositivo móvil. Con este análisis preliminar se presentó la idea al Sr. Walker Verdezoto representante principal de la fundación PROCODIS, estos requisitos se transformaron en la lista de producto del proyecto.

E. LISTA DE PRODUCTO REFINADA

La lista de producto o Product Backlog representa a los requisitos transformados en historias de usuario. Para cada Sprint se tiene una lista de producto el cual ha sido refinado y validado que pueda desarrollarse correctamente. En la Tabla III, se presenta la lista de producto ordenada con base a su prioridad.

TABLA III. Lista De Producto

Código	Nombre	Descripción	Prioridad
HU01	*Diseñar el bosquejo (Mockup) de la interfaz de usuario*	*Se debe crear un bosquejo de la aplicación que permita acceder a todas las funcionalidades rápidamente.*	*Alta*
HU02	*Los usuarios requieren una interface de ingreso a la aplicación*	*La aplicación contará con una pantalla de menú principal para desplazarse a las distintas funcionalidades fácilmente.*	*Alta*
HU03	*Los usuarios requieren una lista de eventos agendados en el calendario*	*La aplicación contará con una pantalla para listar eventos que se tengan agendados en el calendario.*	*Alta*
HU04	*Los usuarios requieren el detalle de un evento seleccionado*	*La aplicación contará con una pantalla que permitirá mostrar el detalle de un evento seleccionado.*	*Alta*
HU05	*Los usuarios requieren una notificación del recordatorio del evento*	*La aplicación contará con una pantalla que mostrará información del recordatorio personalizado de un evento.*	*Alta*
HU06	*Los usuarios requieren notificar de sus eventos agendados a un contacto*	*La aplicación contará con una pantalla que permitirá notificar de un evento agendado a un contacto en específico.*	*Alta*
HU07	*Los usuarios requieren agregar un nuevo contacto*	*La aplicación contará con una pantalla para agregar un nuevo contacto.*	*Media*
HU08	*Los usuarios requieren una pantalla de introducción de la aplicación*	*La aplicación contará con una pantalla que permitirá indicar un paso a paso del uso de las funcionalidades.*	*Media*
HU09	*El administrador requiere una pantalla que permita llenar una encuesta de usabilidad.*	*La aplicación contará con una pantalla que permita llenar una encuesta y enviarla para su registro.*	*Media*
HU10	*Los usuarios requieren una pantalla de configuración de la aplicación*	*La aplicación contará con una pantalla que permita ubicar la configuración e información acerca de la aplicación.*	*Media*
HU11	*Pruebas funcionales y de rendimiento*	*Se deben realizar pruebas funcionales y de rendimiento de la aplicación para validar el correcto funcionamiento de la misma.*	*Media*
HU12	*Pruebas de accesibilidad y usabilidad*	*Se deben realizar pruebas de accesibilidad y uso con usuarios que tengan discapacidad visual*	*Media*
HU13	*Implementar funcionalidad para acceder a reuniones en Zoom desde el detalle del Evento.*	*La aplicación validará si es una reunión de Zoom y permitirá redireccionar a la sala de la reunión.*	*Media*
HU14	*Implementar que la notificación del evento sea enviada al correo del contacto.*	*La aplicación permitirá enviar una notificación al correo del contacto.*	*Media*
HU15	*Implementar funcionalidad por voz en la aplicación móvil.*	*La aplicación permitirá ingresar a todas las funcionalidades por medio de la voz.*	*Media*

F. ARQUITECTURA DE LA APLICACIÓN

Para la representación de la arquitectura se utilizó un diagrama de despliegue UML el cual permite mostrar los componentes que forman parte de la aplicación para su correcto funcionamiento.

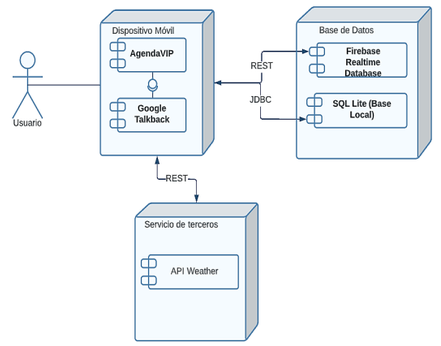


Fig. 3 Arquitectura de la Aplicación

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

En cuanto a la organización del proyecto, se utilizó el patrón de arquitectura de software Modelo Vista Controlador (MVC) el cual permite separar la lógica de la aplicación de la interfaz de usuario, facilitando el mantenimiento y la escalabilidad de la aplicación [16].

En la Figura 4, se puede apreciar la estructura de la aplicación siguiendo el patrón MVC descrito anteriormente, en este patrón se muestra el flujo de datos e instrucciones que existen entre las distintas capas, tomando como base lo mencionado en [17] [18].

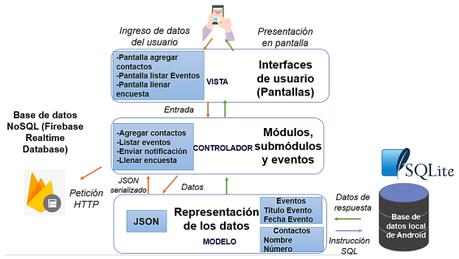


Fig.4 Modelo Vista Controlador de la aplicación móvil

Estas 3 capas se encuentran detalladas a continuación:

- *Modelo (Model):* Es la representación de los datos, contiene los objetos que pertenecen a la lógica del negocio y permite la comunicación con la base de datos. Para almacenar la información de las encuestas se utiliza una base de datos NoSQL alojada en la nube denominada Firebase RealTime Database. Esta base de datos cuenta con una sola estructura denominada Encuestas.
- *Vista (View):* Representa la información a través de los elementos visuales que la componen, es la interfaz con la cual el usuario interactúa. En el presente proyecto se tienen las siguientes interfaces de usuarios:
  - Pantalla de introducción
  - Pantalla de menú principal
  - Pantalla para agregar contactos
  - Pantalla para listar eventos
  - Pantalla detalle de evento
  - Pantalla para enviar notificación
  - Pantalla para llenar encuesta
  - Pantalla acerca de la aplicación
- *Controlador (Controller):* Representa el enlace entre el modelo y la vista, es el responsable de recuperar los datos del modelo, prepararlos y exponerlos hacia la vista. En la presente arquitectura, el controlador representa los módulos y eventos que procesan las interacciones del usuario. Los módulos de la aplicación son:
  - Introducción
  - Menú principal
  - Agregar contactos
  - Listar eventos
  - Enviar notificación
  - Acerca de la aplicación
  - Llenar encuesta

G. EJECUCIÓN DE SPRINTS

Para el presente trabajo se contó con un total de 6 Sprints, con una duración de 2 semanas cada uno. La estimación se la consiguió con base en la experiencia en el desarrollo móvil y la complejidad de las distintas historias, se acogió el estándar de que un Sprint no debe durar más de un mes.

TABLA IV. Planificación Del Lanzamiento

Sprint 1	*Sprint 2*	*Sprint 3*	*Sprint 4*	*Sprint 5*	*Sprint 6*
HU01	*HU04*	*HU07*	*HU10*	*HU13*	*HU11*
HU02	*HU05*	*HU08*	*HU15*	*HU14*	*HU12*
HU03	*HU06*	*HU09*			

El seguimiento de cada Sprint se lo llevó a cabo utilizando la herramienta GitKraken Boards, mediante esta herramienta se listan las historias de usuario por Sprint y se indica sus criterios de aceptación para que estas puedan ser aprobadas al final del Sprint.

A continuación, se describe como ejemplo el proceso de ejecución del Sprint 1, este proceso se repite a lo largo de los siguientes Sprints.

- *Objetivos del Sprint 1:*
  - Diseñar el bosquejo (Mockup) de la interfaz de usuario.
  - Los usuarios requieren una interface de ingreso a la aplicación.
  - Los usuarios requieren una lista de eventos agendados en el calendario.

Fig. 5 Tablero de las historias pertenecientes al Sprint 1

- *Revisión del Sprint 1:*

Al finalizar el Sprint 1 se validan los criterios de aceptación de cada historia y se realiza una presentación del resultado de las mismas, con ello se logra validar el cumplimiento de los objetivos planteados. Se realiza una pequeña retrospectiva donde se tiene como resultado que no existe, de momento, ningún bloqueante o impedimento para el próximo Sprint.

H. USO DE SERVICIOS FIREBASE

Para el almacenamiento de las respuestas de la encuesta de usabilidad, la cual se encuentra integrada dentro la aplicación, se utilizó la base de datos de Firebase (Firebase Realtime Database), en ella cada encuesta cuenta con un identificador único por usuario. Esto puede observarse en la Figura 6.

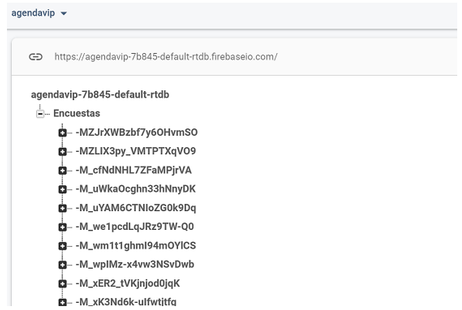


Fig.6 Almacenamiento de respuestas de encuesta de usabilidad

I. PUBLICACIÓN EN LA TIENDA

Para la publicación de la aplicación AgendaVIP en la tienda de Google Play se debió realizar el proceso de creación y pago de una cuenta como desarrollador. Una vez se contó con la cuenta de desarrollador se procedió a subir la aplicación en formato. AAB (Paquete de aplicación de Android) y estar a la espera de su aprobación.

Actualmente, se encuentra publicada en la tienda de Google Play bajo la versión 1.3. La aplicación cuenta con un total de 23 dispositivos activos y se encuentra disponible en un total de 176 países o regiones. Esto se lo puede observar en la Figura 7.

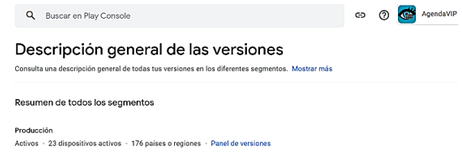


Fig. 7 Publicación en la tienda Google Play

VI. RESULTADOS Y DISCUSIÓN

A. ENCUESTA DE USABILIDAD

En la presente sección, se presentan los resultados de las pruebas de usabilidad y accesibilidad realizadas en el último Sprint. Las pruebas de usabilidad de la aplicación fueron realizadas con los miembros de la fundación PROCODIS, en total fueron 10 personas que apoyaron con las pruebas de la aplicación, las cuales según Nielsen [19] a partir de 5 usuarios los errores encontrados comienzan a repetirse, por lo tanto, 10 usuarios son suficientes para determinar la usabilidad de la aplicación. Una vez culminada las pruebas se solicitó a los usuarios que procedieran a llenar la encuesta de usabilidad.

La encuesta tiene la finalidad de determinar cuál fue la experiencia del usuario al utilizar la aplicación, y si recomendaría su uso a otras personas. A continuación, se presentan las preguntas realizadas y sus respectivas respuestas.

Como se puede observar en la Tabla V, existe un 70% de aprobación por parte de los encuestados respecto a la aplicación. Resultado que llevó a realizar un análisis con los usuarios que realizaron las pruebas y consecuentemente llenaron la encuesta, se consultó el porqué de las respuestas de las preguntas 2, 3 y 4.

TABLA V. Preguntas de encuesta de usabilidad

	Muy buena	*Buena*	*Mala*	*Pésima*
1. ¿Cómo fue su experiencia al utilizar la aplicación?	*40%*	*50%*	*10%*	*0%*
	Si	*No*		
2. ¿La aplicación permite realizar las taras que ofrece?	*70%*	*30%*		
3. ¿La aplicación le es de utilidad y, por lo tanto, planea utilizarla frecuentemente?	*70%*	*30%*		
4. ¿Recomendaría el uso de la aplicación?	*70%*	*30%*		

Con lo cual se logró determinar lo siguiente:

Para la respuesta de la pregunta 2, los usuarios que respondieron que no permite realizar las tareas que ofrece se debe a que hubo una mala interpretación de las funcionalidades de la aplicación. Por ejemplo, en uno de los casos el usuario pensó que la aplicación era

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

un flujo lineal entre el agregar contacto y el enviar notificación. Esto evidenció que debe especificarse con más detalle cuales son las funcionalidades de la aplicación, por ello se realizó esta mejora en las pantallas de introducción. Una vez realizada esta mejora, se procedió nuevamente a validar con los usuarios partiendo desde las nuevas indicaciones de la pantalla de introducción. Los usuarios comentaron que mediante este cambio en la introducción se proporciona mayor información en las funcionalidades de la aplicación y que deja claro el cómo utilizar cada una de ellas de forma correcta.

Para el caso de las respuestas de las preguntas 3 y 4, van muy de la mano con la respuesta de la pregunta 2, ya que como los usuarios no pudieron completar un flujo completo o correcto, entonces es claro que no les sería de utilidad la aplicación ni tampoco podrían recomendarla. Para este caso, se aplicó la misma solución presentada anteriormente, por lo tanto, se consiguió resultados positivos.

B. ANÁLISIS DE ACCESIBILIDAD

Las pruebas de accesibilidad se las realizaron tanto haciendo un barrido mediante la aplicación prueba de accesibilidad como con los usuarios con discapacidad visual, a los cuales se les pidió que realicen una navegación normal por toda la aplicación. A continuación, en la Figura 8 se observa el resultado del análisis realizado.

Fig.8 Resultado del análisis de accesibilidad

Como se puede observar en el análisis final, realizando un recorrido de toda la aplicación se nos presenta que no existe ninguna sugerencia de accesibilidad dentro de la aplicación. Está inspección se la realizó siguiendo un checklist de cumplimiento, aplicando las mejoras descritas en las pautas de accesibilidad de la WCAG 2.1. Estas en su mayoría eran cambios a nivel visual, tales como: contraste en el color del texto con respecto al fondo, etiquetas descriptivas, páginas tituladas y tamaño de elementos seleccionables.

VII. CONCLUSIONES

El interés, la gran acogida y el entusiasmo que mostraron los integrantes de la fundación PROCODIS al enterarse del proyecto, y más aún luego de que ya pudieron probar un producto funcional, demuestra que existe la necesidad de diseñar y desarrollar tecnologías que permitan ser utilizadas por la mayor cantidad de personas independientemente de sus características.

Con base en los resultados conseguidos en la encuesta de usabilidad y a las correcciones posteriormente realizadas y validadas con los usuarios, se pudo constatar que AgendaVIP cumple con su funcionalidad de ser una aplicación de utilidad y accesible para personas con discapacidad visual.

La aplicación aplicación AgendaVIP logró cumplir con las pautas de accesibilidad del estándar WCAG 2.1 consideradas dentro del proyecto, pautas como: texto alternativo (etiquetando todos los elementos disponibles en pantalla), adaptable (agrupando los elementos de tipo texto para su correcta lectura por Google Talkback), distinguible (validando la relación de contraste del texto de 4.5:1), navegación (validando el tamaño mínimo de 48dpx48dp de los botones y titulando cada pantalla) y asistencia en ingreso de datos (colocando etiquetas e instrucciones en la pantalla para ingreso de información del nuevo contacto). El cumplimiento de estas pautas en AgendaVIP se ve reflejado en los resultados de la sección.

Análisis de Accesibilidad

La elección del marco de trabajo Scrum para el desarrollo del artefacto fue acertada, ya que permitió adaptarse a los cambios que surgieron en el desarrollo de la aplicación. Así mismo, permitió mantener una correcta planificación de los requisitos a implementarse y los tiempos de entrega del producto funcional.

El desarrollo del artefacto ayudó a resolver el problema planteado apoyando a las personas con discapacidad visual a poder manejar una agenda personal desde sus dispositivos móviles, les permitió crear recordatorios que les facilite el tener presente sus actividades tanto diarias, como semanales.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

VIII. TRABAJOS FUTUROS

Para futuras versiones de la aplicación se tiene pensado implementar pruebas de accesibilidad automática para lograr un producto de mejor calidad y que siga aportando las mimas e inclusive mejores funcionalidades. . Por temas de la situación actual con el Covid-19, no se pudieron realizar pruebas en persona con los usuarios, por ello se tiene como objetivo poder realizar mejoras a la aplicación móvil las cuales puedan ser probadas de forma presencial y en conjunto con los usuarios finales de la fundación PROCODIS.

Finalmente, como continuación del presente trabajo se plantea el continuar desarrollando aplicaciones accesibles que cumplan con las pautas recomendadas dentro de los estándares de la WCAG 2.1. Con la tecnología en constante avance, cada vez se hace más necesario utilizar dispositivos móviles para realizar ciertas tareas cotidianas e indiscutiblemente las personas con algún tipo de discapacidad forman parte de esa población.

IX. AGRADECIMIENTOS

Quiero agradecer a la fundación PROCODIS y a todos sus miembros por estar siempre presentes y dispuestos a brindar el apoyo necesario para el desarrollo de este proyecto, su experiencia y conocimiento en el uso de la tecnología fue un gran aporte para poder lograr entregar un producto de calidad y más que nada que aporte.

También quiero agradecer al Sr. Walker Verdezoto representante principal de la fundación por permitirme realizar este proyecto con la fundación ya que sin su apoyo el proyecto no se hubiera podido realizar.

REFERENCIAS

[1] Consejo Nacional para la Igualdad de Discapacidades, "Estadísticas de Discapacidad", 2022. [En línea]. Disponible en: https://www.consejodiscapacidades.gob.ec/estadisticas-de-discapacidad/. [Accedido: 12-may-2022].

[2] Primicias EC,"Dos inventos ecuatorianos facilitan la inclusión de las personas ciegas,". [En línea]. Disponible en: https://www.primicias.ec/noticias/tecnologia/inventos-ecuatorianos-inclusion-no-videntes/. [Accedido: 11-oct-2020].

[3] A. Rodriguez, D. De la Cruz, J. Tobar, P. Mejía, N. Paredes y G. Olmedo, "Voice — TOUCH GPS: Navigation and mobility assistant for people with visual disability in Ecuador," 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), 2017, pp. 1-7, doi: 10.23919/CISTI.2017.7975821.

[4] N. P. Landazabal, O. Andrés Mendoza Rivera, M. H. Martínez, C. Ramírez Nates y B. T. Uchida, "Design and implementation of a mobile app for public transportation services of persons with visual impairment (TransmiGuia)," 2019 XXII Symposium on Image, Signal Processing and Artificial Vision (STSIVA), 2019, pp. 1-5, doi: 10.1109/STSIVA.2019.8730263.

[5] PCWorld, "Las mejores apps para organizarse de 2021" [En línea]. Disponible en: https://www.pcworld.es/mejores-productos/software/apps-organizacion-3682549/#toc-3682549-6. [Accedido: 20-jun-2021].

[6] D. Amalfitano, A. R. Fasolino, P. Tramontana, y B. Robbins, "Testing Android Mobile Applications: Challenges, Strategies, and Approaches," in Advances in Computers, vol. 89, Academic Press Inc., 2013, pp. 1–52. [En línea]. Disponible en: https://tinyurl.com/y3kghk8k. [Accedido: 22-sep-2020].

[7] World Health Organization, "Blindness and vision impairment.", 2021. [En línea]. Disponible en: https://www.who.int/en/news-room/fact-sheets/detail/blindness-and-visual-impairment. [Accedido: 10-may-2021].

[8] ISO/IEC, "ISO - ISO/IEC Guide 71:2001 - Guidelines for standards developers to address the needs of older persons and persons with disabilities." [En línea]. Disponible en: https://www.iso.org/standard/33987.html. [Accedido: 6-oct-2020].

[9] ISO, "ISO 9241-171:2008(en), Ergonomics of human-system interaction — Part 171: Guidance on software accessibility." [En línea]. Disponible en: https://tinyurl.com/yyoon78h. [Accedido: 8-oct-2020].

[10] Accessible University, “Defining Accessibility - Accessible University.” [En línea]. Disponible en: http://www.accessibleuniversity.com/accessibility-basics/defining-accessibility. [Accedido: 3-sep-2020].

[11] Google, “Cómo empezar a usar Android con TalkBack - Ayuda de Accesibilidad de Android.” [En línea]. Disponible en: https://tinyurl.com/4ns4ynud. [Accedido: 10-abr-2021].

[12] C. Khawas, y P. Shah, “Application of Firebase in Android App Development-A Study”, International Journal of Computer Applications 179, 2018, doi: 10.14257/ijhit.2014.7.5.29.

[13] W3C, “Web Content Accessibility Guidelines (WCAG) 2.1.” [En línea]. Disponible en: https://www.w3.org/TR/WCAG21/. [Accedido: 10-may-2021].

[14] K. Schwaber y J. Sutherland, “La Guía de Scrum TM La Guía Definitiva de Scrum: Las Reglas del Juego Español,” Scrum. Org, p. 22, 2017. [En línea]. Disponible en: https://www.scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-Spanish-SouthAmerican.pdf. [Accedido: 04-may-2021].

[15] C. Scharff y R. Verma, “Scrum to support mobile application development projects in a just-in-time learning context,” International Conference on Software Engineering, 2010, pp. 25–31, doi: 10.1145/1833310.1833315.

[16] K. Sokolova, M. Lemercier, y L. Garcia, “Android Passive MVC: a Novel Architecture Model for the Android Application Development,”Patterns 2013, pp. 7–12, 2013. [En línea]. Disponible en: https://bit.ly/3iZXbiv. [Accedido: 17-jun-2021].

[17] L. Tian, “A comparison of Android Native App Architecture – MVC , MVP and MVVM,” pp. 57, 2016. [En línea]. Disponible en: https://pure.tue.nl/ws/portalfiles/portal/48628529/Lou_2016.pdf. [Accedido: 14-jul-2021].

[18] I. Sarker y K. Apu, “MVC Architecture Driven Design and Implementation of Java Framework for Developing Desktop Application,” International Journal of Information Technology, vol. 7, no. 5, pp. 317–322, 2014, doi: 10.14257/ijhit.2014.7.5.29.

[19] Jakob Nielsen, “Why You Only Need to Test with 5 Users.”, 2020. [En línea]. Disponible en: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/. [Accedido: 20-jun-2021].

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

AUTHORS

Jaime Crespin

Ingeniero en Sistemas Informáticos y de Computación. Se encuentra trabajando como Ingeniero de Desarrollo en la empresa Cobis.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022
DOI: 10.5281/zenodo.6763281

María Hallo

Docente de la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. MSc. en Informática de la Universidad Notre Dame de la Paix. PhD. en Aplicación de la Informática de la Universidad de Alicante.

LATIN-AMERICAN JOURNAL OF COMPUTING

Published by

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas
Quito-Ecuador

https://lajc.epn.edu.ec/
lajc@epn.edu.ec

July 2022

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2022

Vol IX, Issue 2, July 2022

https://www.epn.edu.ec

QUITO - ECUADOR

LAJC

LATIN-AMERICAN JOURNAL OF COMPUTING

Vol IX, Issue 2,
July 2022

Indexed in: