OIC-CERT
Computer Emergency Response Team

OIC-CERT JOURNAL OF CYBER SECURITY

Volume 5, Issue 1
July 2024

Enhancing the knowledge on cyber security among the OIC member countries

The Organisation of the Islamic Cooperation - Computer Emergency Response Team
www.oic-cert.org

ISSN 2636-9680
eISSN 2682-9266

Published by CyberSecurity Malaysia as the
OIC-CERT Permanent Secretariat

ISSN 2636-9680
eISSN 2682-9266

Editorial Panel

OIC-CERT Journal of Cyber Security

Volume 5, Issue 1
July 2024

Content

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
1 - 10

Cloud Security Maturity Index to Measure the Cybersecurity Maturity Level of Cloud Service Providers in Indonesia

Raden Budiarto Hadiprakoso[1], Hermawan Setiawan[2], I Komang Setia Buana[3]
Herman Kabetta[3], Rahmat Purwoko[4], and Amiruddin[5]
[1-6] State Cyber and Crypto Agency, Jakarta, Indonesia
budiarto.hadiprakoso@bssn.go.id[1], hermawan.setiawan@bssn.go.id[2]
komang.setia@bssn.go.id[3], herman.kabetta@bssn.go.id[4]
rahmat.purwoko@bssn.go.id[5], amiruddin@bssn.go.id[6]

ARTICLE INFO

Article History
Received 31 Jan 2023
Received in revised form 31 Jan 2024
Accepted 20 Mar 2024

Keywords:
Cloud security; cloud security government; KAMI index; maturity model; cloud-security framework

ABSTRACT

Cyberspace has an impact on every aspect of our lives. *Cloud computing* is a innovative cyberspace technology that has established itself as one of the essential resource-sharing platforms for forthcoming on-demand infrastructures and services that enable the internet of things, big data, and software-defined systems/services. Security is more important than ever in a cloud environment. Numerous cloud security models and standards are in place to deal with emerging cloud security concerns. However, these models are primarily reactive rather than initiative-taking and do not give suitable measures to analyze a cloud system's overall security posture. Capability maturity models, which many companies have utilized, provide a practical method to address these issues through management by security domains and security evaluation based on maturity levels. The paper has two goals: first, it provides a review of cyber security, cloud security models and standards, cyber security capability maturity models, and security metrics; second, we propose a cloud security maturity index (CSMI) that extends existing information security models (KAMI index) with a security metric framework. CSMI seeks to provide senior management with a reliable overall security evaluation of a cloud system and to enable security professionals to foresee and identify essential security solutions.

I. INTRODUCTION

The cloud has emerged as the backbone of digitization, empowering governments and businesses to navigate dynamic events, unlock new opportunities, and build resilience for swift recovery [1]. Recent global developments underscore the urgency of digital transformation.

Firstly, the three-year pandemic served as a catalyst, accelerating digitization by seven years globally and ten years in Asia Pacific, according to McKinsey [2]. However, corporations now find implementation more challenging, requiring them to act 20-25 times faster than anticipated [2].

Secondly, the global response to climate change is intensifying. The European Union aims for carbon neutrality by 2050, while China pledges to peak emissions by 2030 and achieve neutrality by 2060 [3]. Digital technology presents a key solution, with the World Economic Forum estimating that Information and Communications Technology (ICT) could save 12.1 billion tons of emissions by 2030, ten times its own sector's footprint [4].

Thirdly, the increasingly complex global economic landscape necessitates resilience in business strategies [5]. Digital technology plays a crucial role here, and the low-carbon economy's resurgence further compels businesses to accelerate their digital transformation initiatives.

ISSN 2636-9680
eISSN 2682-9266

Indonesia exemplifies this trend. In the past five years, cloud computing adoption has surged by 48%, significantly exceeding the global average of 19% [6]. A 2021 Thales survey shows that 80% of Indonesian (Small Medium Enterprise) SMEs and large firms utilize cloud solutions in various forms [7]. Reports indicate Indonesia's active embrace of cloud-based technology: 77% of firms already use it, and 83% believe it aids pandemic survival [8]. During the pandemic, 67% of Indonesian enterprises adopted more cloud solutions, while 64% see hybrid cloud solutions as crucial for resilience [8, 9]. Security remains a primary concern, with credential security and solution-infrastructure compatibility being key considerations for 62% of businesses before the pandemic [10].

Cloud computing Indonesia predicts a (Compound Annual Growth Rate) CAGR of 18.9% growth between 2020 and 2024 [11]. By 2021, 50% of SMEs are expected to see a 20% income increase due to cloud adoption, with a projected $10.7 billion boost to Indonesia's GDP over the next five years [11, 12]. The International Data Corporation survey projects Indonesia's public cloud services market to reach US$1.3 billion by 2025, with a 28.1% CAGR from 2020 to 2025 [12].

Despite this progress, challenges remain. Credential security persists as a critical factor for 64% of Indonesian firms during the pandemic, highlighting growing cybersecurity awareness as enterprises expand their digital footprint [13]. A Center for Strategic and International Studies poll reveals that 69.8% of public organizations in Indonesia still do not utilize cloud services due to data security and privacy concerns, with an additional 33.1% citing uncertainties in the rule of law [11].

Cloud computing's adaptability, network-centric approach, and ease of access have driven its popularity among diverse users [14]. However, the immaturity of security technology deters some service providers from fully embracing it, highlighting the need for investment in this area [14]. Additionally, the distributed nature of cloud data, while offering redundancy for disaster recovery, presents potential security risks as data becomes more susceptible to theft and loss [15]. Other security concerns include inadequate user segregation, identity theft, privilege abuse, and insufficient encryption [15].

This study addresses these challenges by conducting a literature review to assess the current state of knowledge surrounding cloud security concerns and potential solutions. We briefly cover the security challenges in cloud computing and explore general strategies that could lead to solutions. Notably, we propose a maturity index for cloud computing security as a key contribution.

The remaining sections of the paper are structured as follows: Section 2 presents related works, Section 3 describes our research methodology, Section 4 focuses on results and discussion, and Section 5 summarizes our findings and provides recommendations in conclusion.

II. RELATED WORK

Cloud security maturity models play a critical role in helping organizations transition to cloud environments securely. These models provide a structured framework for evaluating the effectiveness of security controls, identifying gaps, and implementing best practices to mitigate risks. This literature review explores existing research and publications on cloud security maturity models, focusing on their development, components, application, and impact.

Existing Cloud Security Maturity Models:

- Cloud Security Alliance (CSA) Standards [17]. The CSA advocates a multi-layered approach using virtual LANs, Intrusion Detection/Prevention Systems (IDS/IPS), and firewalls to safeguard data in transit. They also emphasize data leakage prevention due to the shared underlying infrastructure of virtual networks. Additionally, the CSA recommends robust access management solutions.
- Advanced Cloud Protection System (ACPS) Model [18]: This model enhances cloud resource security by offering various services like network protection against user and CSP data breaches. ACPS employs continuous monitoring by the host platform to mitigate cross-tenant attacks. It also enables behavior-based anomaly detection for virtual machines.

- Information Security Management System (ISMS) [19]: ISMS refers to a comprehensive set of policies for managing information security risk. Paper [19] defines it as a standardized approach that addresses all security aspects from a management perspective. It aligns with ISO standards specifying security design, implementation, operation, and management practices.

Information Security (IS) Evaluation:
Information security (IS) evaluation assesses the effectiveness of security controls in protecting organizational information assets. It estimates security risk levels and prioritizes them based on asset value and potential impact. The primary objective is to assess the implemented security controls within an organization. This involves identifying and assessing system risks, measuring security preparedness based on current technology, and comparing results [20, 21].

Securing Cloud Data:
Authors in [22] propose a security approach for cloud-based data using standard and specialized methods with additional recommended measures. Users can assign a 1-10 rating to data secrecy, availability, and integrity needs. These values are used to calculate a "Sensitivity Rating" for the data. Decentralized cloud storage authentication and access control methods have also been explored [23, 24]. Anonymous authentication allows users to verify their identity without revealing it.

Mitigating Post-Violation Risks:
Security breaches or cancellations of Security Service Level Agreements (SLAs) can expose user assets to significant risk. Authors in [25] propose a risk-aware renegotiation approach to mitigate security risks in such situations.

Gaps and Opportunities:
While extensive research addresses security and privacy concerns in cloud computing, much of it focuses on data security, privacy, authorization, and data integrity (Reference 22). We need to explore unlocking the value of reliable data and accelerating digital transformation in terms of sovereignty, economic development, and cybersecurity for both governments and enterprises.

Significant research has been conducted using the KAMI index concept in both public and private sectors. However, further research is needed on constructing a more specific Information Security Maturity Model for cloud security [26]. Existing models like KAMI tend to be broad and limited in scope. To address this, we propose a Cloud Security Maturity Index (CSMI) model that measures the security level of cloud computing services. This approach complements existing assessments conducted by cloud users, as it focuses specifically on cloud provider security practices.

III. METHODOLOGY

The many characteristics of Cloud computing have made the long-dreamed vision of computing as a utility a reality and will potentially shape the whole IT industry. When deciding whether or not to move into the cloud, potential cloud users would consider factors such as service availability, security, and system performance.

Data protection is a crucial security issue for most organizations. Before moving into the cloud, cloud users need to identify data objects to be protected, classify data based on their implication on security, and then follow the security policy for data protection and policy enforcement mechanisms.

The research method used is the literature study method. This strategy emphasizes sifting through journals, papers, and other study materials to locate pertinent information for the issue at hand. This technique examines publications from renowned publishers such as MDPI, IEEE, and Science Direct. All data collected comes from journals, books, or other sources.

Additional resources discovered through exploratory research that are trustworthy, applicable, and fall within the criteria established for this technique are also included. In order for the material or data included in this research study to be accurate and pertinent, a rigorous method or protocol is followed. The

ISSN 2636-9680
eISSN 2682-9266

protocol used in this literature review approach is based on paper [10] recommendations.
The approach is intended for information system researchers who perform most of their study using a literature review technique.

This methodology guarantees the correctness and dependability of data taken from several sources. This method approach can provide knowledge related to cloud security issues and feasible solutions, cloud security, and general tactics that lead to solutions, frameworks for data security governance, and be able to propose maturity indexes for cloud computing security.

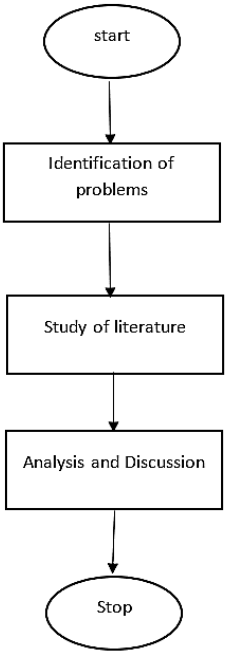

Fig 1. Research Flow

The KAMI Index, developed by the Indonesian government, serves three purposes:

1. **Evaluating Maturity:** It assesses the maturity level of information security management systems (ISMS) within government agencies.
2. **Completeness Assessment:** It measures the completeness of implementation for SNI ISO/IEC 27001:2009, an international standard for ISMS.
3. **Governance Mapping:** It provides a map of the information system security governance landscape within a particular agency.

However, despite its usefulness, the KAMI Index has limitations that necessitate exploring alternative models:

- **Limited Scope:** The KAMI Index primarily offers a basic overview of an agency's information security maturity. It doesn't assess the effectiveness or appropriateness of their ISMS in handling security incidents.
- **Lack of Improvement Guidance:** The Index doesn't provide an improvement plan or recommendations on how to enhance information security practices (protection, maintenance, management, and execution).

These limitations are particularly concerning the recent rise in cyberattacks targeting Indonesia. The escalating cyber threats highlight the critical need for robust information security, a need effectively addressed by well-implemented ISMS.

IV. RESULT & DISCUSSION

This paper proposes a new framework for auditing cloud services, referring to and adopting a framework that categorizes security control activities into three blocks, spanning several domains. CSMI (Cloud Security Maturity Index) is here to assist CSPs in becoming more effective security leaders. It offers a methodical way to evaluate and develop risk management while giving cloud security the respect it merits inside the company.

This framework, called the CSMI (Cloud Security Maturity Index), may be used to level the security dialogue inside your company. It assesses where CSP is now and where the destination is to go. It serves as a guide for CSP to evaluate present and potential partners and vendors. This CSMI framework uses a security domain classification for the cloud model [27], assigning it to each area mentioned in the table below.

TABLE 1: CSMI design domain division

Blocks	Domain
Security	Governance and Enterprise Risk Management
	Security as a Service

Privacy	Data Center Operations
	Information Management and Data Security
	Application Security
	Encryption and Key Management
	Identity and Access Management
	Incident Response, Notification and Remediation
Confidentiality	Legal Issues: Contracts and Electronic Discovery
	Compliance and Audit

The audit process can address one or several domains in a single assessment. An organization must identify its control deficiencies quickly. As such, organizations must understand the effectiveness of their controls and regularly conduct self-audits. Audit findings can help an organization get a complete picture of its compliance and identify deficiencies.

To establish a unified security quality benchmark within an organization, the working group has developed an audit method related to the requirements of the cloud service security (CSS) audit framework.

This CSMI on CSS audit framework may provide detailed security control requirements for CSPs to implement and audit security measures. However, it is not easy to evaluate the effect of these measures beyond their implementation status through audits.

Thus, in addition to auditing, CSPs must measure the impact of their security and privacy protection measures, which requires adequate and feasible cloud security measurement methods and appropriate metrics.

This new framework on measurement of CSS audit framework is mainly done by monitoring and collecting data on key metrics over a while. Organizations can then use the data to analyze and verify changing trends in cloud security across the board. Organizations can understand and evaluate their performance by gathering a sample of metrics.

Regarding NIST SP 800-55r1 and ISO 27004:2016 measurement methods and industry best practices, our new CSS audit framework proposes the following fundamental principles for metric development:

1. Measurable activities: Security management activities must be measurable.
2. Repeatable process: Measurements can be repeated over a certain period.
3. Obtainable data: The established measurement method can obtain adequate data.
4. Comparable results: The data obtained through measurement can be used for comparison and trend analysis.
5. Guidance for management: Analysis of measurement data supports decision-making and helps improve management.

After defining measurement principles, CSPs can design related management metrics and methods following this new framework on cycle measurement and improvement of the CSS audit framework [28]:

One Star: Initial Level: This is the security's first and minimal level of maturity. The CSP has implemented the security controls defined by ISO/IEC 27001 on a basic level, which provides a management framework for implementing an information security management system (ISMS). The security management processes and tools are not developed systematically but are implemented based on practices.

• Two Stars: Basic Level: To have compliance with the two-star security assurance of CSMI, some more security-specific tools/techniques will be required to be adopted by the organizations for more secure software development. The CSP's security controls cover most controls defined in level-1 basic requirements of the new KAMI regarding the CSS audit framework. The CSP has developed and maintained formal processes and provided related tools.

• Three Stars: Intermediate Level: At this level, security must be planned and implemented very preciously in all the processes at every stage of the development life cycle. The CSP complies with the review and measurement methods defined by the new framework regarding the CSS audit framework and conducts regular assessments and improvements of cloud security governance capabilities.

• Four Stars: Advanced Level: This is an advanced level of security. The CSP widely uses mature management technologies and tools and has industry-leading capabilities in

ISSN 2636-9680
eISSN 2682-9266

certain key business domains. The cloud security governance system is constantly monitored, measured, evaluated, and optimized.

• Five Stars: Leading Level: This is the final and five stars level in which the development organization will offer the software with maximum achievable security. The CSP widely uses mature security management technologies and tools and can develop innovative solutions. The CSP has developed innovative security governance methodologies.

TABLE 2: Maturity Level and Description

Maturity Level and Description	
Initial	• The CSP has established a security management system based on widely accepted industry standards (such as ISO/IEC 27001) and provided basic security management capabilities. • The CSP has implemented the security controls defined by ISO/IEC 27001 on a basic level, which provides a management framework for implementing an information security management system (• The security management processes and tools are not developed in a systematical manner but are implemented based on practices. • Basic information security management documents are in place.
Basic	• The CSP has established a cloud service cyber security and compliance governance system based on the 3CS framework. • The CSP's security controls cover most controls defined in level-1 basic requirements of the new KAMI regarding cloud service security audit framework. • The CSP has developed and maintained formal processes and provided related tools. • The CSP has released formal management documents and conducted regular maintenance through formal processes.
Intermediate	• The CSP has the capability to meet most level-2 basic requirements defined by the new KAMI regarding cloud service security audit framework and has provided certain process automation supported by mature tools. • The CSP complies with the review and measurement methods defined by the new KAMI regarding on cloud service security audit framework and conducts regular assessment and improvement of cloud security governance capabilities.
Advanced	• The CSP has the capabilities to meet most level-2 basic requirements defined by the new KAMI regarding on cloud service security audit framework and meet most level-2 supplementary requirements. • The CSP widely uses mature management technologies and tools and has industry-leading capabilities in certain key business domains. • The cloud security governance system is constantly monitored, measured, evaluated, and optimized.
Leading	• The CSP has the capabilities to meet all level-2 basic requirements defined in the new KAMI regarding on cloud service security audit framework as well as all level-2 supplementary requirements. • The CSP widely uses mature security management technologies and tools and is able to develop innovative solutions. • The CSP has developed innovative security governance methodologies.

V. CONCLUSION

This research, informed by both literature and web searches, explores the advantages, disadvantages, and challenges associated with a country's transition to cloud computing. One potential drawback lies in vendor lock-in, where contract termination fees can create revenue losses.

This research emphasizes the importance of robust cloud security for countries choosing suitable cloud service providers aligned with their goals. Cloud technology can foster innovation and knowledge creation, but vendor lock-in presents a significant concern.

As a new technology adopted by countries for market growth, cloud security is paramount due to the storage of sensitive data. Fortunately, cloud security systems effectively encrypt and verify transmitted information before decryption.
This paper examines existing security standards used by the Indonesian government to enhance security and raise awareness of national vulnerabilities.

While offering valuable findings, the paper recognizes several limitations:

1. Context-Specific Adaptability: While acknowledging the importance of context in cloud security maturity models, the paper lacks a detailed exploration and implementation of this concept. Future research could delve deeper into the impact of organizational context (industry, size, deployment model) on maturity model design and application.

2. Validation and Empirical Testing: The proposed cloud security maturity index lacks extensive empirical validation in real-world settings. Future research could conduct case studies and empirical studies to assess the effectiveness and applicability of such models across diverse contexts, providing valuable insights into their practical utility and limitations.

3. User-Centric Perspectives: While user perspectives are briefly mentioned, the paper lacks in-depth exploration of user-centric aspects like usability, user experience, and organizational culture. Future research could incorporate user-centric design principles into maturity models to enhance usability and adoption, considering the diverse needs and preferences of stakeholders involved in cloud security management.

Effective cloud security can significantly impact state-owned programs. Future research could explore relevant regulations and laws, as well as the impact of cloud computing on national organizational structures.

In conclusion, the cloud security provided will be able to impact the programs owned by the state. In the future, further research can be carried out regarding the regulations and laws that must be complied with by cloud security; and, how the cloud affects the organizational structure of countries.

VI. REFERENCES

[1] M. Hamad, A. Kuwaiti, and T. M. al Kaissi, "A Comprehensive Reconsideration of Cloud Security Approach," *OIC-CERT Journal of Cyber Security*, vol. 4, no. 1, p. 51, 2022.

[2] McKinsey, "Capture a digital transformation's value today," 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value (accessed Jan. 28, 2023).

[3] P. Friedlingstein *et al.*, "Global carbon budget 2019," *Earth Syst Sci Data*, vol. 11, no. 4, pp. 1783–1838, Dec. 2019, doi: 10.5194/ESSD-11-1783-2019.

[4] S. Panchiwala and M. Shah, "A Comprehensive Study on Critical Security Issues and Challenges of the IoT World," *Journal of Data, Information and Management*, vol. 2, no. 4, pp. 257–278, Dec. 2020, doi: 10.1007/S42488-020-00030-2.

[5] D. Angamuthu and N. Pandian, "A Study of the Cloud Computing Adoption Issues and Challenges," *Recent Advances in Computer Science and Communications*, vol. 13, no. 3, pp. 313–318, Aug. 2020, doi: 10.2174/2213275911666181114142428.

[6] F. D. Mobo, "Cloud Computing Security, Privacy and Forensics: Issues and Challenges Ahead," *International Journal of Recent Trends in Engineering and Research*, vol. 4, no. 3, pp. 10–13, Mar. 2018, doi: 10.23883/IJRTER.2018.4083.XWPNA.

[7] Thales, "The Challenges of Data Protection in a Multicloud World," 2022.

[8] L. Vishwakarma, R. Shukla, and S. Pavani, "SECURITY RELATED ISSUES AND CHALLENGES IN CLOUD ENVIRONMENT," *Wutan Huatan Jisuan Jishu*, vol. 17, no. 7, 2021, Accessed: Jan. 28, 2023. [Online]. Available: https://cmdpgcollege.ac.in/Uploads/SECURITY%20RELATED%20ISSUES%20AND%20CHALLENGES%20IN%20CLOUD_2021037080626.pdf

[9] S. Panchiwala, M. S.-J. of Data, I. and Management, and undefined 2020, "A comprehensive study on critical security issues and challenges of the IoT world," *Springer*, Accessed: Jan. 28, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s42488-020-00030-2

ISSN 2636-9680
eISSN 2682-9266

[10] A. S. AlAhmad, H. Kahtan, Y. I. Alzoubi, O. Ali, and A. Jaradat, "Mobile cloud computing models security issues: A systematic review," *Journal of Network and Computer Applications*, vol. 190, p. 103152, Sep. 2021, doi: 10.1016/j.jnca.2021.103152.

[11] A. Gui, Y. Fernando, M. S. Shaharudin, M. Mokhtar, I. G. M. Karmawan, and - Suryanto, "Cloud Computing Adoption Using TOE Framework for Indonesia's Micro Small Medium Enterprises," *JOIV : International Journal on Informatics Visualization*, vol. 4, no. 4, p. 237, Dec. 2020, doi: 10.30630/joiv.4.4.458.

[12] L. Sanny, A. Hamada, A. Prameswari, and A. Setiawan, "Effects of Social Media Marketing in Cloud Kitchen Towards Online Platform in Indonesia," in *2022 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Sep. 2022, pp. 367–371. doi: 10.1109/iSemantic55962. 2022.9920470.

[13] A Bayunata, "Analysis Of Minimum Design Security For Private Cloud In Indonesia Using NIST Sp 800-30 To Fulfill ISO 27001," *Master of Information Technology*, 2023, Accessed: Jan. 28, 2023. [Online]. Available: https://thesis.sgu.ac.id/ index.php/ots/article/view/3994

[14] D. Moh. and W. Millary Agung, "Utilization EOS Platform as cloud-based GIS to analyze vegetation greenness in Cirebon Regency, Indonesia," *Journal Of Information Technology And Its Utilization*, vol. 3, no. 1, pp. 1–4, 2020, Accessed: Jan. 28, 2023. [Online]. Available: http://karya.brin.go.id/id/eprint/13806/

[15] F. Murni, M. Heikal, A. Suhaimi, and M. Khaleel, "Intention to adopt cloud accounting: A conceptual model from Indonesian MSMEs perspectives," *koreascience.or.kr*, vol. 7, no. 12, pp. 749–759, 2020, doi: 10.13106/jafeb .2020.vol7.no12.749.

[16] N. Santoso, A. Kusyanti, H. Puspa, and Y. April, "Trust and Security Concerns of Cloud Storage: An Indonesian Technology Acceptance," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 6, pp. 453–458, 2018, doi: 10.14569/IJACSA.2018.090662.

[17] Cloud Security Alliance, "Cloud Security Alliance's Top Threats to Cloud," Jun. 07, 2022. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/ (accessed Jan. 29, 2023).

[18] F. Lombardi and R. di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113–1122, Jul. 2011, doi: 10.1016/j.jnca.2010.06.008.

[19] H. Hambali and P. Musa, "Analysis Of Governance Security Management Information System Using Index Kami In Central Government Institution," *Angkasa: Jurnal Ilmiah Bidang Teknologi*, vol. 12, no. 1, Mar. 2020, doi: 10.28989/angkasa.v12i1.563.

[20] Y. Fernando, S. Achmad, and A. Gui, "Leveraging business competitiveness by adopting cloud computing in Indonesian creative industries," *Int J Bus Inf Syst*, vol. 32, no. 3, pp. 364–392, 2019, doi: 10.1504/IJBIS.2019.103082.

[21] M. N. Sahid Ramadhan, A. Amyus, A. N. Fajar, S. Sfenrianto, A. F. Kanz, and M. S. Mufaqih, "Blood Bank Information System Based on Cloud Computing In Indonesia," *J Phys Conf Ser*, vol. 1179, no. 1, p. 012028, Jul. 2019, doi: 10.1088/1742-6596/1179/1/012028.

[22] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[23] C. J. Vijaya, C. Narasimham, and P. Sai Kiran, "Authentication and Authorization Mechanism for Cloud Security," *Int J Eng Adv Technol*, vol. 8, no. 6, pp. 2072–2078, Aug. 2019, doi: 10.35940/ijeat. F8473.088619.

[24] T. Alam, "Cloud Computing and its role in Information Technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, Feb. 2020, doi: 10.34306/itsdi.v1i2.103.

[25] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and S. X. Shen, "Joint Pricing and Security Investment in Cloud Security Service Market with User Interdependency," *IEEE Trans Serv Comput*, vol. 15, no. 3, pp. 1461–1472, May 2022, doi: 10.1109/TSC.2020.2996382.

[26] N. B. Muhammad and M. Bazzi, "Advances in Cloud Computing: Security Issues and Challenges in the Cloud," in *2022 5th International Conference on Information and Computer Technologies (ICICT)*, Mar. 2022, pp. 110–116. doi: 10.1109/ ICICT55905.2022.00027.

[27] G. Mateescu and M. Vlădescu, "Auditing Hybrid IT Environments," 2014. [Online]. Available: www.ijacsa.thesai.org

[28] S. K. Pandey, "Security Vigilance System through Level Driven Security Maturity Model," *International Journal of Computer Science, Engineering and Information Technology*, vol. 2, no. 2, pp. 11–17, Apr. 2012, doi: 10.5121/ijcseit.2012.2202.

ISSN 2636-9680
eISSN 2682-9266

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
11 - 18

Evidence-Based Critical Infrastructure Intelligence and Resilience Actions Against Cyber Cybersecurity Inequities

Ernest Tambo[1,2,5], Kennedy Okorie[1,3], Ngo Tappa Tappa[1,3,4] Narcisse Ngouamo[1,3], Hoberlin Fotsing Sadeu[1] , and Patience N Njinyah[1,3]
[1]Africa Disease Intelligence, Preparedness and Response, Yaoundé, Cameroon
[2]School of Public Health, Faculty of Medicine, Universite des Montagnes, Cameroon
[3]Department de Sante Publique, Faculté de Médecine, Université de Douala, Cameroon
[4]Association for Equity, Resilience and Wellbeing in Africa (APERA)
[5]Center for Leadership in Global Health Equity, University of Global Health Equity, Kigali, Rwanda
tambo0711@gmail.com

ARTICLE INFO

Article History
Received 25 Oct 2023
Received in revised form 31 Jan 2024
Accepted 27 Feb 2024

Keywords:
Cyber-defense, cyber-resilience, partnership, data sharing, vulnerability, cyberattacks

ABSTRACT

There is an emerging trend of cyber inequity between countries, corporates and organizations, evolving technological transition, current cyber-skills and workforce shortage that calls for an urgent needs and importance of building a better local and global cybersecurity ecosystem. The scale and sophistication of cyberattacks/threats and cybercrimes landscape continue to fuel the lucrative nature of ransomware, automation disruption, theft of intellectual property and data business concerns. There is urgent need to enhance cyber resilience and defense systems by prioritizing and investing in improving cyberdefence and cyber-resilience postures of governments and critical firms, as variety of complex systems and technologies are becoming increasingly vulnerable to attacks, incidents and threats/crimes. The article assesses critical infrastructure and population data vulnerabilities in shaping cyberdefence and cyber-wellness in targets domains against cyberthreats, attacks and cybercrime globally and in Africa particularly. We documented that increasing ransomware, extortion and ubiquitous phishing supply chain attacks are now all commonplaces. Our findings showed that financial services, mining and healthcare, travel and personal information and identity are the most affected domains. The most vulnerable African countries were namely Ethiopia, Nigeria, South Africa, Algeria, Rwanda and Kenya. Phishing was by far the most prevalent crime with growing prevalence of others. Scaling up cybersecurity and compliance solutions requires a coordinated and dedicated commitment and investment to cyberdefence in Africa. Proactive multisectorial partnership and data sharing collaboration is a potential game changer and resiliency to keep cyber-threats on surveillance check, priorities settings and aligned national actions plans. Sharping shared focus and bringing parties and stakeholders together is essential in building crucial evidence-based cyberdefence and cybersecurity, vulnerability monitoring and compliance solutions. Our results are discussed in improving data-driven or evidence-based cybersecurity intelligence, cyberdefence data sharing protection and improved public–private partnership those are essential building blocks in increased regulatory enforcement, legislative reforms actions and protection measures including digital trust, cyber-inclusive future and resiliency against cyberattacks vulnerabilities, losses and damages. Timely and continuous cyber information triage, analysis and shared cybersecurity and cyberdefence intelligence such as artificial intelligence and deep machine learning potential applications from multisource have immense potential to enrich more contextual and actionable defensive

ISSN 2636-9680
eISSN 2682-9266

capacities including threat detection and mitigation intelligence, cyber information equitable sharing, early waning and response systems.

I. INTRODUCTION

Hastening internet permeability coupled with COVID-19 infodemics has given rise to an upsurge in digital transformation across the globe. Cyberattacks are proliferating causing turmoil among organization in nations affecting health, financial and mining firms tempering with privacy integrity. Essentially, cyberattacks or threat could be seen as any form of un authorized entry or jeopardy of financial integrity, cessation of ongoing processes, or soiling to the eminence of an intuition as a results of a breakdown of its information technology (IT) systems, as spell out by the Institute of Risk Management (IRM) (1).

Cybersecurity involves the clustering of technologies, procedures and applications constructed to ensure integrity of information processing systems from intrinsic or extrinsic blackmail and unwarranted entrance(1,2).The Global Risk Report by the World Economic Forum, estimated squandered financial resources due to cyber threats is estimated as US$ 6 trillion as of 2021(3,4) . Digitalization of trade and business operations through the Internet of Things (IoT), Artificial intelligence (AI), cloud computing, mobile, block chain, and upcoming technological revolutions, cyber threat is ingrained and extremist (4). This section should provide the background on the context of the problem. Justify and rationalize the importance of the research. State the problem statement and the matters to be discovered and the steps the researcher took to fill the gaps or improvements to the situation such as the research objectives, scope, solutions and the contribution of the findings.

II. THE GROWING TREND OF CYBERATTACKS

Cyberattacks are a growing geopolitical risk, becoming larger, more intricate and more relentless. They are a significant threat to firms, organizations and national security. The United States of America is facing a widespread ransomware issue, and the US government is demanding stricter safeguards to help protect against such threats. The European Parliament website was made inaccessible for several hours in November 2022, with a pro-Kremlin group claiming responsibility for the cyberattack. Moldova's government suffered a data breach as recently as January 2023, and Australia's second-largest telecom company, Optus, suffered a data breach in September 2022 (1,4). The digitization of critical national infrastructure (CNI or health data) means that many essential services, including power grids, water supply networks and transportation systems, are increasingly vulnerable to cyberattacks. A successful cyberattack on any of these systems can have severe consequences, including loss of life and economic damage. The repercussions of persistent cyberattacks and cybercrimes could have a wide-reaching impact on financial markets and the economy. Government networks, private sector networks and infrastructure are all susceptible to hacking and espionage. International cooperation to effectively address cyberattacks is challenging given the complex geopolitical relationships between many countries, and climate-conflict linked poverty vicious cycle. As wars and geopolitical tensions rise between some of the world's major powers igniting critical and targeted structures and data cyberattacks vulnerabilities and corporate criminalities losses and damages (2,5)

The lack or inefficiency of cyberspace local and international laws enforcement against infringements resulted closely to $7 billion of financial loss, and about $15 million stored data were revealed through breaches 2021-2022, compared to over 300 businesses attacks since June 2022 to date in United States of America. For example, both Uganda telecoms and the Banking sector found themselves embedded in crisis due to hackers gaining access to Uganda money network services of which became more solicited as a result of COVID-19 pandemic. Nearly, estimated $3.2 million lost as results of hackers utilizing approximately 2000 Subscriber Identity Module Cards in establishing mobile money payment scheme. The subsequent largest

healthcare provider was targeted by a cyber-attack amidst COVID-19 pandemic, incapacitating 6500 private healthcare bed

provider, giving them no options than to revert to manual backup systems (5,6,7).

However, building evidence-based resilient and robust cyberdefence and cybersecurity partnership and data security guidelines to sharing intelligence against critical infrastructure cyberattacks and vulnerabilities summing up remain considerably low in African nations (2,3,5,6,7).. One of the most predominant puzzle regarding cyberdefence and cyber-wellness safety in policies and regulations are not adequately integrated across the board in Africa and worldwide. Cybersecurity requires continuous investment in an area where best practices are a moving target due to its evolutionary, adversarial and asymmetric nature and mostly scarcity of evidence research on cybersecurity leadership on market opportunities. Better understanding of competitive advantage and potential risk categories and factors for resilience building and strategic allocation of resources.

This article assesses shared cyber-attacks and crime vulnerabilities trends in harnessing evidence-based mutlisectorial/transnational cyberdefence/cybersecurity partnerships and data sharing intelligence and collaboration, comprehensive cyberdefence prevention and mitigation strategies implementation in targets critical infrastructure and populations in Africa and worldwide.

III. IMPLEMENTING CYBERSECURITY AND CYBERDEFENCE PARTNERSHIP, DATA SHARING POLICY AND GOVERNANCE FRAMEWORK

Our findings reported an increasing malware attacks, cybercrimes is now of a dynamically and recurrently threat surfacing out with new digital initiatives and a series of weaponry technological innovations in other to cause more disruption and damage to users of essential digital infrastructures at massive scale. There is a necessity in involving civil society in nationwide cyber security blueprint and policy more than ever. Civil society ensures proper dissemination of national cyber security strategies, so that it can be broadly read, popularly acknowledge, so that intuitions like state, private enterprises, and other actors are held liable for misconduct(11).Fostering collaboration with government, so as to permit the identification of susceptible sectors and facilitating in incident response and recovery solutions is of utmost importance in safeguarding essential national infrastructure(11).

These major cyber-attacks reported come in different forms, such as espionage attempts, Denial-of-Service (DoS) attacks and ransomware attacks. For Example, a cyberattack that disrupts hospital services can have serious consequences, such as delaying emergency care, cutting off supplies and services, or causing the death of patients. The increased digital device and network activities have attracted many hackers that seek to steal personal information or disrupt services. In addition, cybercriminals have also attempted to compromise hospitals and research centers on cybersecurity and cyberdefence research needs is substantial and not limited to professionals (12).

This requires public and private partnership and cyberspace collaboration and governance in other to boosting participative cybersecurity investment and promoting threat or crime information intelligence sharing, adhering to international cybersecurity principles, norms and best practices. Harnessing effective and efficient mitigation and adaptation methods to cyber-incidents response plans. In addition, strengthening evidence-based cyber maturity and reactiveness, in early real time, resilient and robust detection and response to threats or crimes. There is a need to create a cybersecurity ecosystem and platforms where global users of all ages need to be educated and be aware of the risks of the cyber world and must be prepared to fend off-hackers that attempt to infiltrate their networks and personal accounts. Mobile, digital and cloud-based-internet designers and users should avoid giving out personal information or opening doubtful websites and application software (13) (Table 1)

ISSN 2636-9680
eISSN 2682-9266

TABLE 1: Summary of cyberattacks and crimes across Africa and worldwide

Cybercrimes and attacks	**Key solutions and recommendations**
Non-payment and non-delivery	▪ Promotion of Public private partnership ▪ Building cross sectorial collaboration ▪ Enhanced data protection and data security ▪ Enhanced email and document encryption ▪ Fast tracking cyber resilience digital signing ▪ Proactivity and more efficient recovery tactics ▪ Computer biometric and cryptographic solutions ▪ Personal information protection on social media
Personal data breach	
Phishing, whaling and pharming	
Extortion	
Identity theft and password attack, email frauds, social media frauds	
Malware, ransomware, soyware, Trojans, deepfakes	
Denial of services and Tunneling	
Online scam and cryptocurrency	
Cyber espionage	
Clickjacking	
Banking frauds	
Trafficking	
Malacious email and website	
Major malware attacked by countries in 2022	**Percentage (%)**
Ethiopia	62%
Algeria	59%
Burundi	57%
Rwanda	46%
Kenya	41%
Nigeria	40%
Zimbabwe	40%
Ghana	39%
Zambia	38%
South Africa	36%
Uganda	36%

IV. STRENETHENING LOCAL AND REGIONAL CYBERDEFENCE AND CYBERSPACE CAPACITY BUILDING

Setting up the enabling law enforcement for law enforcement to proactively defend and counter cyber threats against law enforcement networks and critical technologies security, safety and protection environment including intellectual property rights (IPR) is essential for cybersecurity mobile and digital to Artificial intelligence services delivery, telecommunication and social media services, monitoring information system building capacity. Also, offer safety compliance support to companies and stakeholders in securing their infrastructure, transactions and online services, application and data confidentiality, with a wider range of solutions and technical assistance. The growing sophistication of cyber-threats and attacks require more preparation including capacity building and training for collective defense, crisis management and cooperative security, aligning with international laws, enhance local and regional resilience and provide a platform for advocacy and political consultation to collective action.

Cyber related crime lansdscape is likely to continue and evolve, from critical infrastructures and businesses email compromise, ransomware, data theft and extortion, impersonations, scams, phishing / smishing (including “quishing” through QR codes), credential stuffing and extortions globally. While health, financial services and retail are likely to remain key focus areas, we also see increased risk for our essential services / critical infrastructure. We are yet to see an attack that has a prolonged impact on the operational integrity of critical assets. This is perhaps one of our biggest risks, more serious in many respects than a cyber incident affecting data alone.

Although building and maintaining cyberattacks to cyberspace are complex, destructive and becoming ever more frequent,

continuous adaptation to the evolving threat an crime landscape require strengthening African countries cybersecurity and cyberdefence posture. Mauritius is usually quoted and advertence in the globe due to its cyber security capabilities , its judicial and functional infrastructure, its nationwide cyber security agency (CERT-MU), its national capacity building and cognizance leadership, and the implication both public and private sectors in these endeavors. Mauritius is top ranking regarding African nations and 14th worldwide,

by the ITU Global Cybersecurity Index (GCI) released in 2018 (14).
It has set up a National Disaster Cybersecurity and Cybercrime Committee that includes both public and private sectors and facilitates the monitoring, control, and transmission of decisions during cyber crises. Mauritius is one of the eight African countries to have ratified the Malabo, with which their Computer Misuse and Cybercrime Act is aligned, along with the Budapest convention on cybercrime. Mauritius has constructed a principal portal to register cyber incidents and a security intelligence center to identify and invigilate mischievous traffic instantaneously to ensure cyber security readiness nationwide (15).

V. EVIDENCE-BASED AND ACTIONABLE CYBERDEFENCE INTELLIGENCE AND RESILIENCE SYSTEM

Our findings showed that as health care personnel's and financial organizations are becoming more reliant on dedicated digital infrastructures and data-driven medical procedures , an abrupt cyberattack and subsequent shutdown can yield disastrous consequence in patient care, client and the enterprise/intuition all together. Cybersecurity, data security, and information assurance policies are of utmost importance for clinical laboratories to entirely be ready for potential cyber- attacks today and in the future as these is unavoidable in the digital age transformation (12)

Artificial intelligence (AI), deep machine learning (DML) technological innovations data mining and interpretation are which can be tailored into algorithms producing reliable predictive analytics, and for decisions making policies and practices can help in evidence-based decision support systems, efficient risk management, pattern recognition, cyber incident clustering, fore casting, malware identification and data safeguarding. For example, AI-based cybersecurity enabled application networks could sense vulnerabilities (bugs) and provide adequate threat response or quarantine there by strengthening, information system network security resilience.

Hence, further AI and DML-linked cybersecurity and cyber-wellness research and innovation (R&I) is no now the new normal in the digital era, to distillate the technological revolutions of AI-powered cybersecurity policies, due to its tremendous computing and processing power, tailoring complex algorithms for efficient security ecosystem, while addressing ethical and legal AI and digital issues and concerns.

VI. Combating critical infrastructures cyberattacks and cybercrimes

Recently, the development of the Nigeria's Cybersecurity Policy and Strategy, independent professional bodies like the Nigeria Computer Society and the Cybersecurity specialist/Experts Association of Nigeria provided feedback.

These clusters, whose enrollment intersect with public, private, and nonprofit actors as well as other decision makers from Nigeria's diaspora, enabling an upgraded technical skills, data sovereignty, and civic responsibility (11).

Practical and sustainable information logistics and dissemination management systems can be valuable in strengthening and securing transactions and deliveries. There is also need to explore vulnerabilities of electronic vehicle; electronic and grid security control units where attackers could potentially take control of these computer system or communication systems and manipulate the vehicle behavior causing accidents and other dangerous situations.

ISSN 2636-9680
eISSN 2682-9266

VII. BUILDING COLLECTIVE,EQUITABLE AND SUSTAINABLE CYBERDEFENCE OR CYBER-RESILIENCE SYSTEMS

Our findings showed an escalating number of cyber threats, eventually leading to difficulties to judicial prosecutors and legislative bodies in ensuring cyber security across the board and chiefly on critical infrastructures and cvber-equity.

Strengthening cyber-resilience requires investment in research, development, and the importation of international cyber security norms, which have proven its effectiveness for proper dissemination to national local regional sectors of the digital ecosystem justice.

African nations should proactively update and ratify a regional and national cybersecurity strategy to provide a comprehensive legal and framework, guidelines and mechanism on threat/crime surveillance, identification and incidence response for adequate protection and security of critical infrastructure.

These strategies should stipulate a nation-wide response plan during cyber-attacks, coupled with proper withdrawal strategies from cyber threats, ensuring both public and private sector should be capable of normal functioning even in the advent of sudden data loss during cyberattacks thereby, ensuring sustainability of quality cybersecurity service delivery in responses to cyber-attacks.

VIII. CONCLUSION

There is an emerging trend of cyber inequity between countries, corporates and organizations, evolving technological transition, current cyber-skills and workforce shortage leading toe increasing cyberattacks. Weak data and information privacy and rights protections concerns remain challenged due to ineffective national security, watchdog transparency and transnational enforcement laws and regulatory measures across Africa and worldwide. Leveraging on shared cybersecurity and cyberdefence collective partnership and governance framework, knowledge exchange, experiences and capabilities. This is crucial for proactive, resilient and sustained informed decisions and response actions against potential cyberattacks, crimes and vulnerabilities worldwide. Improving cybersecurity and other digital/electronic devices compliance guidelines, and or published data records, accounts and database long-term retention. It is necessary to develop and maintain policies and procedures to ensure high quality and better protection rights and security of individual, company and national security against unreasonable searches and seizure, and respect business rights.

IX. REFERENCES

[1] Kabanda G, Chingoriwo T. A Cybersecurity Culture Framework for grassroots levels in Zimbabwe. Orient.J. Comp. Sci. and Technol; Vol. 14(1-2-3) 17-34 (2021). Available from: https://bit.ly/3J1mQB2. W. P. Risk, G. S. Kino, and H. J. Shaw, "Fiber-optic frequency shifter using a surface acoustic wave incident at an oblique angle," *Opt. Lett.*, vol. 11, no. 2, pp. 115–117, Feb. 1986.

[2] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. Cybersecurity data science: an overview from machine learning perspective, 2020. Journal of Big Data. https://doi.org/10.1186/s40537-020-00318-5.

[3] World Economic Forum. Global risk report. 2020. https://www.weforum.org/reports/the-global-risks-report-2020. Accessed 1st August 2022.

[4] Shevchenko PV, Jang J, Malavasi M, Peters GW, Sofronov G, Trück S. The nature of losses from cyber-related events: risk categories and business sectors. J Cybersecurity. 1 janv 2023;9(1):tyac016.

[5] Allison A, Chatzilia A, Canham D. et al. Cyber risk executive summary. Technical Report. London: Institute of Risk Management, 2014b.

[6] Allison A, Chatzilia A, Canham D. et al. Cyber risk resources for practitioners. Technical Report. London: Institute of Risk Management, 2014a.

[7] Statista (2022) Africa: number of internet users in 2022, available at https://www.statista.com/statistics/505883/numberof- internet-users-in-african-countries/.

[8] Daniel Batty & Ethan Mudavanhu , (23 JUNE, 2022).The State of Cybersecurity in Africa: The Chinese Effect.

[9] Lesotho Times (2022), National Assembly approves cybercrime bill, available at National Assembly approves cyber-crime bill – Lesotho Times (lestimes.com).

[10] ITU (2021), Are African countries doing enough to ensure cybersecurity and internet safety, available at https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/.

[11] Abdul-Hakeem Ajijola and Nate D.F. Allen (March 8, 2022). African Lessons in Cyber Strategy. https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/.

[12] Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, et al. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med. 4 janv 2023;8(1):145-61.

[13] Saleous H, Ismail M, AlDaajeh SH, Madathil N, Alrabaee S, Choo KR, Al-Qirim N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digit Commun Netw. 2022 Jun 23. doi: 10.1016/j.dcan.2022.06.005. Epub ahead of print. PMID: 35765301; PMCID: PMC9222023.

ISSN 2636-9680
eISSN 2682-9266

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
23 - 34

Comparative Analysis of eKYC and 2FA in Implementing PADU Database System to Strengthen Digital Identity Security

Nor Izham Subri[1], Abdul Ghafur Hanafi[1], Mohd Affendi Ahmad Pozin[2]
Faculty of Business and Management Science, Kolej Universiti Islam Perlis (KUIPs), Perlis, Malaysia[1]
Faculty of Business & Communication, Universiti Malaysia Perlis (UniMAP), Malaysia[2]
***izham@kuips.edu.my**

ARTICLE INFO

Article History
Received 30 Jan 2024
Received in revised form 31 Jan 2024
Accepted 14 Feb 2024

Keywords:
electronic Know Your Customer, eKYC, PADU Database, Two-Factor Authentication, 2FA

ABSTRACT

As digital transactions and online interactions become integral components of modern society, ensuring robust digital identity security is paramount. This study addresses this imperative by investigating the effectiveness of two authentication methods, electronic Know Your Customer (eKYC) and Two-Factor Authentication (2FA), within the context of the PADU (Pangkalan Data Utama) Database System. The study employs a retrospective and exploratory research design, relying on secondary data sources for analysis. Through a non-experimental approach, existing information is examined from primary secondary data sources such as scholarly articles, government reports, and industry publications. Additionally, datasets from reputable repositories are accessed to gather statistical information aligned with the objectives. The comparative analysis method evaluates the efficacy of eKYC and 2FA, focusing on criteria such as scalability, user-friendliness, and regulatory compliance. The findings aim to provide policymakers, database administrators, and digital service providers with actionable recommendations to enhance digital identity security within the PADU Database System.

I. INTRODUCTION

In an era dominated by rapid technological advancements and an ever-expanding digital landscape, the imperative to fortify digital identity security stands as a critical necessity. As individuals and organizations increasingly rely on digital platforms for communication, transactions, and information sharing, safeguarding sensitive data against cyber threats becomes paramount. This study endeavours to address this pressing need through a focused investigation into the comparative efficacy of two prominent authentication methods, electronic Know Your Customer (eKYC) and Two-Factor Authentication (2FA), within the implementation of the PADU (Pangkalan Data Utama) Database System.

The escalating frequency and sophistication of cyber-attacks underscore the vulnerability of digital identities, necessitating a proactive approach to security measures. The introduction of PADU represents a pivotal step toward achieving unified and efficient data management within public agencies. However, the efficacy of this database system hinges on the robustness of the authentication mechanisms integrated into its framework.

eKYC emerges as a technology-driven authentication method, relying on advanced biometric and document verification processes to establish and verify individual identities. On the other hand, 2FA employs a multi-layered approach, requiring users to provide two distinct forms of identification – typically something they know (e.g., a password) and something they possess (e.g., a mobile device).

ISSN 2636-9680
eISSN 2682-9266

The implementation of the PADU database system in Malaysia has raised concerns about its security features, particularly in the user registration processes and the lack of multi-factor authentication. The system, which is intended to act as a central database hub for the country, has been criticized for potential vulnerabilities that could be exploited by cybercriminals. Specifically, the absence of multi-factor authentication has been highlighted as a weakness, as it only requires an identity card number and password for login, which can be easily compromised. These concerns have led to privacy and security issues, especially in light of previous data breaches in the country. Despite the government's assurances of comprehensive security measures, the lack of certain security features has led to scepticism and opposition from a portion of the Malaysian population. The concerns raised underscore the importance of robust security measures in the implementation of digital identity systems such as eKYC and to safeguard against potential cyber threats. Economy, with the potential to generate billions of dollars in revenue and create thousands of jobs.

This study seeks to conduct a meticulous comparative analysis of these two authentication methods, with a specific focus on their application within the PADU Database System. By evaluating the strengths, weaknesses, and contextual appropriateness of eKYC and 2FA, we aim to provide valuable insights into the most effective means of enhancing digital identity security. The outcome of this study is poised to inform policymakers, database administrators, and digital service providers on strategically reinforcing the PADU Database System and, by extension, contributing to the broader discourse on secure digital identity management in our interconnected world.

II. RELATED WORK

A. Introduction to Digital Identity Security

Digital identity security is a critical facet of contemporary technological landscapes, as individuals, businesses, and governments engage in an increasing array of online activities. The evolution of digital identities has been paralleled by a growing recognition of the need to safeguard these identities against malicious threats and unauthorized access. According to [1], the proliferation of cyber-attacks targeting personal and organizational data has underscored the vulnerabilities inherent in traditional authentication methods.

The concept of digital identity encompasses the unique set of attributes, credentials, and personal information associated with an individual within the digital realm [2]. As individuals conduct financial transactions, access confidential information, and communicate over digital platforms, the importance of ensuring the integrity and security of digital identities becomes paramount [3]. Cybercriminals continually adapt their tactics to exploit weaknesses in existing security measures, emphasizing the dynamic and evolving nature of the digital threat landscape [4].

In light of these challenges, the literature highlights the necessity for robust digital identity security frameworks to mitigate the risks associated with identity theft, unauthorized access, and data breaches. Existing study [5] underscores the need for multi-layered authentication methods that extend beyond traditional username-password combinations, as these have proven susceptible to various forms of exploitation.

Moreover, the rise of interconnected systems and the Internet of Things (IoT) further amplifies the importance of secure digital identities. As noted by [4], the increasing interconnectivity of devices necessitates comprehensive security measures to protect not only personal information but also the broader ecosystem of interconnected digital entities.

Moreover, the rise of interconnected systems and the Internet of Things (IoT) further amplifies the importance of secure digital identities. As noted by [1], the increasing interconnectivity of devices necessitates comprehensive security measures to protect not only personal information but also the broader ecosystem of interconnected digital entities.

The introduction to digital identity security establishes the foundational understanding of the challenges posed by the evolving digital landscape. The need for effective

authentication mechanisms is evident, prompting a deeper exploration of specific methods, such as eKYC and 2FA, within the context of implementing the PADU Database System.

B. Authentication Methods in Digital Identity Security

In contemporary digital environments, ensuring robust security measures for digital identities is paramount. Authentication methods play a crucial role in safeguarding sensitive information and preventing unauthorized access [6]. Various authentication mechanisms are employed to verify the identity of users, including traditional methods like passwords and PINs, as well as more advanced approaches such as biometrics, multi-factor authentication (MFA), and cryptographic keys [7. These methods serve to fortify the authentication process by requiring users to provide multiple forms of identification, thereby enhancing the overall resilience of digital identity security. The adoption of such multifaceted authentication techniques reflects an ongoing commitment to mitigating the risks associated with unauthorized access, identity theft, and other cybersecurity threats [8]. As the digital landscape continues to evolve, the exploration and integration of innovative authentication methods remain crucial for maintaining the integrity and confidentiality of digital identities.

C. Pengkalan Data Utama (PADU) Database System

PADU Database System in Malaysia serves as a critical platform with the primary objectives of enhancing the efficiency of government service delivery, optimizing the utilization of limited resources, and empowering the social system through economic upliftment [9]. PADU strives to achieve these goals by consolidating and streamlining data, thereby improving the overall performance of government services. By reinforcing the judicious use of limited resources, PADU contributes to effective resource management, ensuring that public funds are utilized efficiently. Moreover, the implementation of PADU aims to empower the social system by fostering economic well-being among the populace. This is accomplished by addressing socio-economic disparities, meeting the needs of the people, and fostering balanced development [10]. Ultimately, PADU stands as a key component in the Malaysian government's commitment to narrowing socio-economic gaps, promoting citizen welfare, and achieving holistic national development.

D. What Is eKYC and How Does it Work.

The process of (eKYC) has emerged as a significant technological advancement for businesses to perform customer identity verification in a digital environment. This alternative approach to the traditional process, which relied on physical documents, has transformed onboarding rules and regulations for businesses. The KYC process has become more complex and must now not only meet regulatory compliance but also cater to the changing customer expectations. eKYC leverages the power of technology to provide businesses with a more agile, scalable, and reliable method of carrying out KYC, thereby serving as an effective solution to the current challenges.

KYC, short for Know Your Customer, is a process of identifying and verifying the identity of a person or entity as part of a transaction in a regulated industry or before and during a financial relationship. This process is crucial in various industries, particularly financial services, and is required by law in many countries across the globe, including the US, the EU, and the UK.

KYC can be mandatory when opening a bank account, applying for a loan, trading securities, purchasing insurance, using online gambling services, or requesting a credit card, among other situations. The purpose of KYC is to enable financial institutions to confirm the identity of their clients and assess their level of risk based on their previous and current financial activities. It also plays a significant role in anti-money laundering (AML) due diligence.

Electronic KYC (eKYC) differs from traditional KYC in the way customer information is collected and verified. While KYC may involve offline procedures such as requesting and checking physical documents,

ISSN 2636-9680
eISSN 2682-9266

eKYC uses digital technology to achieve the same objective. With eKYC, the compliance risk assessment can be carried out without the need for either party to meet physically or exchange physical documents. This process represents a significant step forward in protecting both businesses and society from fraud, terrorism, and other illegal activities.

Fig 1: 10 step EKYC process

E. The Two-Factor Authentication (2FA)

The Two-Factor Authentication (2FA) constitutes a security protocol designed to augment identity verification by requiring users to provide two distinct forms of authentication before accessing a system, account, or application [11]. In contrast to conventional single-factor authentication methods reliant on passwords or PINs, 2FA incorporates a dual-layered approach, typically categorized as something known (e.g., a password), something possessed (e.g., a mobile device or security token), or something inherent (e.g., biometric data). Following the entry of a password, users are prompted to supply a second form of identification, which may involve receiving a one-time code via SMS, email, or a dedicated authentication app, or utilizing a physical device like a security token. By mandating two independent factors, 2FA significantly bolsters security, mitigating risks associated with password theft, phishing, and unauthorized access [12].

(2FA) and (eKYC) are critical components in bolstering digital security and verifying user identities in online transactions [13]. 2FA adds an extra layer of protection by requiring users to provide two distinct forms of identification before accessing accounts or systems. This typically involves a combination of something the user knows (e.g., a password) and something they have (e.g., a mobile device generating a one-time code). On the other hand, eKYC leverages digital technology to streamline and enhance the traditional Know Your Customer (KYC) process, which involves verifying the identity of individuals during financial transactions. Through eKYC, user identities are electronically verified, often utilizing biometric data, government-issued IDs, or other digital credentials. The integration of 2FA and eKYC not only fortifies security by minimizing the risks of identity theft and unauthorized access but also facilitates smoother and more efficient digital transactions, contributing to a robust and trustworthy online environment.

Feature	eKYC (Electronic Know Your Customer)	Two-Factor Authentication (2FA)
Purpose	Identification and verification in online transactions.	Enhancing security by requiring two different authentication factors.
Process	Electronic submission of identity documents, biometric verification, and background checks.	Two different authentication factors: knowledge (password), possession (e.g., mobile device), and/or biometric factors.
Use Cases	Financial transactions, digital services for user authentication.	Securing logins, transaction verification, access to accounts/systems.
Advantages	Enhanced security, streamlined onboarding and authentication.	Increased security with an additional layer, versatile implementation.
Challenges	Privacy concerns, legal and regulatory compliance.	User experience, dependency on specific devices for certain methods.
Implementation Areas	Financial sector, online platforms, digital services.	Across various online accounts, financial transactions, system access.
Security Layers	Enhances security in identity verification processes.	Adds an extra layer of security to login or access processes.
Dependency on Devices	May involve the use of various electronic devices.	Requires possession of specific devices for certain 2FA methods.

III. METHODOLOGY

The study design for this study will employ a comparative case study approach to investigate and analyze (eKYC) and (2FA) systems. A comparative case study is a strategy that allows for the in-depth examination of multiple cases to identify similarities, differences, and patterns across them [14]. In

this context, the cases will involve the implementation and performance of eKYC and 2FA systems in various settings.

This study employs a retrospective and exploratory research design, relying on secondary data sources for the analysis of existing information [15]. Our approach is non-experimental, centered around the examination of pre-existing data rather than the collection of new information through direct observation or experimentation. Primary secondary data sources include scholarly articles, books, government reports, industry publications, and academic works relevant to the topic, forming the foundation for the literature review and theoretical framework [15]. Additionally, datasets and databases from reputable repositories, such as governmental agencies, international organizations, and academic institutions, will be accessed to gather statistical information, trends, and historical data aligned with the objectives.

The data collection process involves a systematic search and retrieval of pertinent secondary data from digital databases, libraries, and online repositories. Keyword searches, inclusion/exclusion criteria, and citation analysis are employed to identify information directly contributing to the study's focus. Data selection criteria prioritize relevance, currency, and reliability, with an emphasis on recent and reliable information from reputable sources.

The analysis phase entails synthesizing and interpreting the collected secondary data. Within the Service-Oriented Architecture (SOA) framework, the analysis phase involves a thorough synthesis and interpretation of the collected secondary data. Qualitative data, such as narrative findings, undergo thematic analysis to extract key insights and discern emerging trends. Ethical considerations remain paramount, emphasizing accurate source citation and strict adherence to the terms and permissions outlined by the original data providers within the SOA ecosystem.

Limitations of this study include potential biases in original data sources, variations in data collection methodologies across studies, and the inability to address certain questions better suited for primary data collection. To enhance credibility and validity, the study employs triangulation of findings from multiple secondary sources and critically evaluates the quality and reliability of each source.

A. Comparative Analysis Framework

In this study, a qualitative analysis will be an integral component of the comparative framework employed to assess the effectiveness and nuances of eKYC and 2FA within the context of the PADU Database System. The qualitative analysis aims to provide a nuanced understanding of the subjective aspects, user experiences, and contextual factors associated with the implementation of these authentication methods.

B. Qualitative Criteria

The qualitative criteria for the comparative analysis will include factors such as user-friendliness, perception of security, and contextual appropriateness within the PADU Database System. Through in-depth interviews with key informants, including digital identity experts, policymakers, and database administrators, qualitative data will be gathered to assess how well eKYC and 2FA align with the specific requirements and challenges of the PADU framework.

C. Thematic Analysis

Thematic analysis will be employed as the primary qualitative analysis method. This involves identifying, analyzing, and reporting patterns (themes) within the data, providing insights into commonalities and differences across the experiences and perspectives of stakeholders. Open coding will be applied to categorize data into initial themes, followed by axial coding to establish connections and relationships between these themes.

D. User Experience Evaluation

User experience, a vital aspect of digital identity security, will be qualitatively assessed through participants' narratives and feedback. Participants' perceptions of the ease of use, intuitiveness, and overall satisfaction with eKYC and 2FA will be explored. By delving

ISSN 2636-9680
eISSN 2682-9266

into user experiences, the study aims to uncover practical insights into the human factors influencing the adoption and acceptance of these authentication methods.

E. Contextual Relevance

The qualitative analysis will also explore the contextual relevance of eKYC and 2FA within the broader implementation of the PADU Database System. It will seek to understand how well these authentication methods align with the system's architecture, data integrity requirements, and the specific needs of public agencies utilizing the PADU framework.

F. Cross Verification with Quantitative Data

Qualitative findings will be cross-verified with SOA Framework to ensure a comprehensive and well-rounded understanding of the comparative analysis. This triangulation of data sources aims to strengthen the validity of the study's conclusions and provide a more robust foundation for evidence-based recommendations.

The qualitative analysis within the comparative framework is designed to capture the rich and nuanced aspects of eKYC and 2FA implementation, shedding light on user perspectives, contextual considerations, and potential areas for improvement within the PADU Database System. Through a qualitative lens, this study aims to contribute valuable insights to the ongoing discourse on digital identity security.

IV. FINDINGS & DISCUSSION

A. Criteria for Comparative Analysis using SOA for Services

Comparison of eKYC and 2FA in table form based on the service criteria:

Criteria	eKYC	2FA
Introduction and Operational Duration	Introduced in the early 2000s; Over two decades operational	2FA methods date back to the late 20th century; Over three decades operational
Maturity and Adoption Rate	Matured and widely adopted; Rapid adoption in financial, telecom, and government sectors	Mature and widely adopted; Increased awareness and integration across online services
Technological Advancements	Leverages advanced technologies like AI, machine learning, and biometrics	Evolved from hardware tokens to include biometrics; Ongoing advancements to enhance security and user experience
Regulatory Impact	Heavily influenced by financial regulations, AML, and KYC requirements	Influenced by data protection regulations and industry-specific compliance standards
Global Reach	Widely implemented globally; Adapted to diverse legal frameworks	Ubiquitous across online platforms with global accessibility; Varies based on standards
Evolution in User Experience	Initially faced challenges in user acceptance due to privacy concerns; Continuous improvements in biometric technology	Improved over time; Introduction of mobile app-based methods; Aim to make 2FA more seamless
Integration Challenges Over Time	Initially faced integration complexities; Improved with the adoption of secure protocols	Historically faced interoperability issues and varied authentication methods; Improved through user education and standardization
Service Standards and Industry Practices	Adheres to industry-specific standards and regulatory guidelines; Development of best practices through industry collaboration	Adheres to standards set by industry bodies and data protection regulations; Evolution of shared industry practices

This table provides a concise comparison of eKYC and 2FA based on the mentioned service criteria

B. Criteria for Comparative Analysis using SOA for Best Practices

Comparison of eKYC and 2FA based on the "Best Practice" criteria:

Criteria	eKYC	2FA
Data Security Best Practices	Adopts best practices for secure storage and processing of sensitive data	Implements encryption, secure token generation, and secure communication protocols
User Privacy Best Practices	Incorporates privacy measures in handling biometric data and personal information	Focuses on protecting user privacy by minimizing data exposure and secure authentication methods

Criteria	eKYC	2FA
Regulatory Compliance Best Practices	Strict adherence to AML, KYC, and other financial regulations; Stays informed and complies with evolving regulatory requirements	Complies with data protection laws and industry-specific regulations; Regularly updates practices to meet changing compliance standards
Continuous Monitoring and Auditing	Implements continuous monitoring of identity verification processes; Conducts regular audits to ensure compliance and security	Regularly monitors authentication processes for anomalies; Conducts audits to assess the effectiveness of 2FA implementation
User Education Best Practices	Provides clear communication to users about the eKYC process and the importance of identity verification	Emphasizes the importance of 2FA to users; Offers educational resources to promote awareness and understanding
Adaptability to Emerging Technologies	Adapts to emerging technologies such as AI and machine learning for improved accuracy	Integrates with new authentication methods and technologies to stay ahead of evolving security threats
Industry Collaboration for Standards	Engages in industry collaboration to establish and adhere to best practices and standards	Participates in industry forums to contribute to the development and adherence of 2FA best practices
User Experience Optimization	Strives for a balance between security and user convenience; Invests in user-friendly interfaces	Focuses on improving user experience by introducing mobile app integrations and push notifications; Aims for seamless 2FA implementation
Incident Response Best Practices	Has a well-defined incident response plan in case of security breaches; Ensures swift and effective response to incidents	Establishes a robust incident response plan to address any unauthorized access or compromise; Takes immediate action in case of security incidents

This table provides a comparison of eKYC and 2FA based on best practices, encompassing data security, user privacy, regulatory compliance, monitoring and auditing, user education, adaptability to emerging technologies, industry collaboration, user experience optimization, and incident response practices.

C. Criteria for Comparative Analysis using SOA for Process

Comparison of eKYC and 2FA based on the "Process" criteria:

Criteria	eKYC	2FA
Identity Verification Process	Utilizes biometric authentication, document verification, and facial recognition for thorough identity verification	Requires users to provide two independent factors, such as a password and a temporary code, for authentication
Onboarding Process	Streamlines customer onboarding through digital document submission and biometric verification	Involves users setting up an additional layer of authentication during account creation, often using a mobile app or code
Authentication Methods	Relies on advanced technologies like AI, machine learning, and biometrics for accurate authentication	Offers various methods including time-based one-time passwords (TOTP), SMS codes, and biometric verification
User Interaction and Experience	Initial challenges in user acceptance; Improvements in biometric technology to enhance user experience	Evolved user interaction; Improved through mobile app integrations and push notifications for a more seamless experience
Regulatory Compliance Process	Heavily influenced by financial regulations; Adheres to AML and KYC requirements; Compliance is a critical factor	Influenced by data protection regulations and industry-specific compliance standards; Compliance is crucial for securing personal information
Integration Challenges Process	Initially faced integration complexities due to diverse regulatory requirements; Improved with secure protocol adoption	Historically faced interoperability issues and varied authentication methods; Improved through user education and standardization
Technological Infrastructure Process	Requires robust digital infrastructure for secure storage and processing of sensitive data	Integrates with existing authentication systems and databases; Requires secure communication protocols and encryption
Scalability and Future Readiness Process	Adaptable to emerging technologies and evolving regulations; Scalability considerations for large volumes	Scalable to accommodate growing user bases; Integration with new authentication methods and technologies
Incident Response Process	Has a well-defined incident response plan; Ensures swift and effective response to security breaches	Establishes a robust incident response plan; Takes immediate action in case of security incidents; Regularly updates response processes

This table provides a comparison of eKYC and 2FA based on the process criteria, encompassing identity verification, onboarding, authentication methods, user

ISSN 2636-9680
eISSN 2682-9266

interaction, regulatory compliance, integration challenges, technological infrastructure, scalability, and incident response processes.

D. Criteria for Comparative Analysis using SOA for Users

Comparison of eKYC and 2FA based on the "Users" criteria:

Criteria	eKYC	2FA
User Adoption and Acceptance	May face challenges due to concerns about privacy and data security	May face resistance due to additional steps during login; User education crucial for acceptance
Accessibility for Users	Requires user cooperation during identity verification processes	Adds an extra layer during login, potentially affecting accessibility; Improves with user-friendly interfaces
User Education and Awareness	Critical to address privacy concerns and educate users about the eKYC process	Essential to educate users about the importance of 2FA, the added security layer, and ease of use
User Satisfaction	Dependent on the ease of the identity verification process; Improves with user-friendly interfaces	Influenced by the user experience during authentication; Improved satisfaction with seamless integration
User Convenience	Strives for a balance between security and convenience; Focus on user-friendly interfaces	Aims to provide secure authentication without compromising user convenience; Push for seamless 2FA implementation
User Privacy Considerations	Incorporates measures to address privacy concerns related to biometric data	Focuses on protecting user privacy by minimizing data exposure and ensuring secure authentication methods
User Feedback Integration	Integration of user feedback to enhance the eKYC process and overall experience	Incorporates user feedback to improve 2FA methods, ensuring a more user-friendly and effective authentication process
User Resistance Challenges	May face resistance due to concerns about sharing biometric data	Historical resistance due to additional steps during login; Overcoming user inertia is a challenge
User-Friendly Interfaces	Strives to provide interfaces that are intuitive and user-friendly	Focuses on developing interfaces that enhance user experience during the authentication process
Mobile App Integration	Mobile app integration for document submission and biometric verification	Utilizes mobile apps for generating codes, enhancing 2FA accessibility and user experience

This table provides a comparison of eKYC and 2FA based on user-related criteria, including adoption, accessibility, education, satisfaction, convenience, privacy considerations, feedback integration, resistance challenges, user-friendly interfaces, and mobile app integration.

E. Criteria for Comparative Analysis using SOA for Platform

Comparison of eKYC and 2FA based on the "Platform" criteria:

Criteria	eKYC	2FA
Platform Integration	Integrates into various platforms such as financial services, telecommunications, and government services	Integrated across a wide range of online platforms, including banking, email, social media, and secure applications
Industry-Specific Platforms	Adapted to industry-specific platforms with compliance to regulatory standards	Implemented across diverse industries, each with specific security and authentication requirements
Global Platform Accessibility	Accessible on a global scale, adapting to diverse legal frameworks and regional regulations	Ubiquitous globally, with variations based on regional standards and the nature of online services
Cross-Industry Applicability	Applicable across different industries, providing identity verification services	Applicable in various sectors, enhancing security for online banking, social media, and e-commerce
API Compatibility	Compatible with secure APIs to ensure data exchange and integration with third-party systems	Requires API compatibility to seamlessly integrate with different online platforms and applications
Cloud Integration	Often leverages cloud infrastructure for secure storage and accessibility	Can integrate with cloud-based authentication services to enhance scalability and accessibility
Mobile Application Support	Supports mobile applications for document submission, biometric verification, and user interaction	Leverages mobile applications for generating codes, enhancing accessibility, and user experience during 2FA
Open-Source Integration	Limited instances of open-source implementations due to security and regulatory considerations	Some 2FA methods have open-source implementations, allowing customization and integration into various platforms

Criteria	eKYC	2FA
Integration with Government Systems	May integrate with government systems for citizen identification and public service accessibility	Implemented in government systems for secure access to sensitive information and citizen authentication
Financial Platform Integration	Widely integrated into financial platforms for customer onboarding and compliance verification	Commonly integrated into online banking platforms for an additional layer of security during login

This table above provides a comparison of eKYC and 2FA based on platform-related criteria, including integration into various industries, global accessibility, cross-industry applicability, API compatibility, cloud integration, mobile application support, open-source integration, integration with government systems, and financial platform integration.

The integration of eKYC and 2FA within the PADU Database System demonstrates a cohesive and streamlined process, enhancing the overall efficiency and security of the system. The interoperability between eKYC and 2FA ensures a seamless user experience, facilitating swift identity verification and providing an additional layer of security through dual-factor authentication [16]. This integration aligns with the system's objectives of safeguarding sensitive information and complying with regulatory standards, particularly those pertaining to identity verification and data security.

The findings indicate that the PADU Database System places a significant emphasis on user-friendly interfaces to ensure accessibility and ease of use [17]. The integration leverages cloud infrastructure, enhancing accessibility and availability for users across diverse geographical locations [18]. While the integration showcases scalability to accommodate a growing user base, challenges related to user adoption are recognized. Hence, user education and awareness campaigns are considered crucial to overcoming potential resistance and encouraging the widespread adoption of the enhanced security measures implemented through eKYC and 2FA.

In conclusion, the integration of eKYC and 2FA within the PADU Database System represents a well-designed and efficient approach to identity verification and authentication. The system's commitment to security, regulatory compliance, and user experience forms a robust foundation, with ongoing considerations for scalability and adaptability to emerging technologies [19]. Despite challenges in user adoption, the findings suggest a comprehensive and future-ready solution for the secure management of citizen information within a government-operated database system.

The integration of Electronic Know Your Customer (eKYC) and Two-Factor Authentication (2FA) within the PADU Database System demonstrates a cohesive and streamlined process, enhancing the overall efficiency and security of the system. The interoperability between eKYC and 2FA ensures a seamless user experience, facilitating swift identity verification and providing an additional layer of security through dual-factor authentication. This integration aligns with the system's objectives of safeguarding sensitive information and complying with regulatory standards, particularly those pertaining to identity verification and data security.

The findings indicate that the PADU Database System places a significant emphasis on user-friendly interfaces to ensure accessibility and ease of use. The integration leverages cloud infrastructure, enhancing accessibility and availability for users across diverse geographical locations. While the integration showcases scalability to accommodate a growing user base, challenges related to user adoption are recognized. Hence, user education and awareness campaigns are considered crucial to overcoming potential resistance and encouraging the widespread adoption of the enhanced security measures implemented through eKYC and 2FA.

In conclusion, the integration of eKYC and 2FA within the PADU Database System represents a well-designed and efficient approach to identity verification and authentication. The system's commitment to security, regulatory compliance, and user experience forms a robust foundation, with

ISSN 2636-9680
eISSN 2682-9266

ongoing considerations for scalability and adaptability to emerging technologies. Despite challenges in user adoption, the findings suggest a comprehensive and future-ready solution for the secure management of citizen information within a government-operated database system.

TABLE 1: Findings and Implications

Findings	Implications
Seamless Integration of eKYC and 2FA	Enhanced efficiency and security in the PADU Database System.
Enhanced Security Measures	Strengthened protection against unauthorized access and data breaches
Efficient User Onboarding	Quick and accurate verification of user identities during onboarding.
Regulatory Compliance	Alignment with regulatory standards, ensuring data security and privacy.
User-Friendly Interfaces	Positive user experience and accessibility within the system.
Adoption Challenges and User Education	Emphasis on the need for educational initiatives to encourage adoption
Scalability and Future Readiness	Capability to grow with a user base and adapt to emerging technologies
Cloud Integration for Accessibility	Improved accessibility and availability through cloud infrastructure
Overall Robust System Foundation	A well-designed system prioritizing security, compliance, and scalability.

This table highlights key discoveries and their implications, providing a quick overview of the integration of eKYC and 2FA in the PADU Database System.

The integration of eKYC and 2FA within the PADU Database System introduces several challenges and considerations that warrant careful attention. Foremost among these challenges is the potential resistance from users encountering for the first time [20]. Overcoming this initial hesitancy necessitates comprehensive user education and awareness campaigns, emphasizing the added security benefits of 2FA. Addressing user concerns is crucial for fostering widespread acceptance and utilization of the enhanced security measures.

Privacy concerns emerge as a significant consideration, particularly in the context of eKYC, which involves the processing of sensitive biometric data [21]. Recognizing and effectively mitigating these concerns require the implementation of robust privacy measures and transparent communication strategies. Striking a delicate balance between ensuring user privacy and meeting regulatory compliance standards is paramount to maintaining user trust and system integrity. Moreover, as the integration evolves, ongoing compliance monitoring becomes imperative to align with changing regulatory frameworks, ensuring sustained adherence to standards.

The integration process itself presents challenges, notably the initial complexities arising from diverse regulatory requirements [22]. Continuous efforts to streamline integration through the adoption of secure protocols and a proactive approach to evolving regulations are essential considerations. Additionally, the system must address the inherent resistance to change that user may exhibit when confronted with alterations to established onboarding processes or the introduction of new security measures. This challenge can be mitigated by implementing change management strategies, gathering user feedback, and implementing gradual rollouts to facilitate a smoother transition.

In conclusion, the successful integration of eKYC and 2FA in the PADU Database System requires a nuanced approach to address challenges related to user adoption, privacy, integration complexities, scalability, user experience, resistance to change, and compliance monitoring. A meticulous consideration of these challenges ensures that the system is not only secure and compliant but also user-friendly and adaptable to the evolving landscape of identity verification and authentication technologies.

V. CONCLUSION

In summary, this study delved into the integration dynamics of eKYC and 2FA within the PADU Database System, shedding light on crucial aspects of security, user experience, and regulatory compliance. The seamless integration process showcased a sophisticated dual-layer authentication system, fortifying the PADU Database System against unauthorized access and aligning with its core objective of preserving sensitive information. Additionally, the incorporation of eKYC streamlined the user onboarding process, ensuring swift and

accurate identity verification during registration. The study also underscored the significance of user-friendly interfaces and accessibility considerations, emphasizing the system's commitment to providing an intuitive experience for a diverse user base.

However, challenges related to user adoption and privacy concerns were acknowledged, signifying the need for targeted user education and transparent communication practices. These challenges notwithstanding, the study recognized the integration's scalability and future readiness, affirming the system's ability to adapt to evolving technologies and accommodate a growing user base. Overall, the findings serve as a valuable resource for policymakers, system administrators, and stakeholders, guiding ongoing enhancements and reinforcing the enduring efficacy of identity verification and authentication processes within the government operated PADU Database System.

VI. ACKNOWLEDGEMENT

We, the authors, would like to express our highest appreciation to the RMIC of Perlis Islamic University College (KUIPs) for their efforts and contributions in making this study a success.

VII. REFERENCES

[1] Green, J. (2022). Cybersecurity Challenges in the Digital Age. *International Multidisciplinary Journal of Science, Technology & Business*, *1*(4), 19-23.

[2] Royer, D., Deuker, A., & Rannenberg, K. (2009). Mobility and identity. In *The Future of Identity in the Information Society* (pp. 195-242). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*, *26*(1), 109-128.

[4] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11.

[5] Crihan, G., Craciun, M., & Dumitriu, L. (2022). Hybrid Methods of Authentication in Network Security. *The Annals of "Dunarea de Jos "University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics*, *45*(1), 7-7.

[6] Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*, 317-348.

[7] Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges. *International Journal of Advanced Computer Science and Applications*, *14*(1).

[8] Marasco, E., & Albanese, M. (2021). FingerPIN: an authentication mechanism integrating fingerprints and personal identification numbers. In *Computer Vision and Image Processing: 5th International Conference, CVIP 2020, Prayagraj, India, December 4-6, 2020, Revised Selected Papers, Part I 5* (pp. 500-511). Springer Singapore.

[9] PADU (2024) https://www.padu.gov.my/

[10] Krishna, B., & MP, S. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Information & Computer Security*, *29*(5), 737-760.

[11] Bhanderi, D., Kavathiya, M., Bhut, T., Kaur, H., & Mehta, M. (2023, March). Impact of Two-Factor Authentication on User Convenience and Security. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 617-622). IEEE.

[12] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4), 208-220.

[13] Sonawane, S. S., & Motwani, D. (2023, October). Blockchain-Powered FinTech: Shaping the Future of Indian Industries. In *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1-7). IEEE.

[14] Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study.

[15] Harris, H. (2001). Content analysis of secondary data: A study of courage in managerial decision making. *Journal of Business Ethics*, *34*, 191-208.

[16] Punjabi, H. (2016). Innovative Payment Systems-Core to India's E-Finance Revolution. *BVIMSR Journal of Management Research*, *8*(1).

ISSN 2636-9680
eISSN 2682-9266

[17] Petrie, H., & Bevan, N. (2009). The evaluation of accessibility, usability, and user experience. *The universal access handbook*, *1*, 1-16.

[18] Xia, J., Yang, C., Liu, K., Gui, Z., Li, Z., Huang, Q., & Li, R. (2015). Adopting cloud computing to optimize spatial web portals for better performance to support Digital Earth and other global geospatial initiatives. *International Journal of Digital Earth*, *8*(6), 451-475.

[19] Gelb, A., & Metz, A. D. (2018). *Identification revolution: Can digital ID be harnessed for development?* Brookings Institution Press.

[20] Björnfot, P., Bergqvist, J., & Kaptelinin, V. (2018). Non-technical users' first encounters with robotic telepresence technology: an empirical study of office workers. *Paladyn, Journal of Behavioral Robotics*, *9*(1), 307-322.

[21] Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. *European business organization law review*, *20*, 55-80.

[22] Kostova, T., & Zaheer, S. (1999). Organizational legitimacy under conditions of complexity: The case of the multinational enterprise. *Academy of Management review*, *24*(1), 64-81.

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
35 - 42

Unveiling Vulnerabilities: Development IoT-Enabled Health Bracelets Without Security Measures

Mohamad Adrian Mohd Fuaad[1], Qairel Qayyum Muhamad Ridhuan[1], Wan Muhammad Alif Firdaus Wan Hanapi[1], Shelena Soosay Nathan*[1,2],
[1]Center for Diploma Studies, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
[2]ITecH Focus Group, Center for Diploma Studies, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
***shelena@uthm.edu.my**

ARTICLE INFO

Article History
Received 30 Jan 2024
Received in revised form 31 Jan 2024
Accepted 26 Jun 2024

Keywords:
Wearable device; healthcare, internet of things; security, privacy

ABSTRACT

The integration of Internet of Things (IoT) technology to strengthen the health bracelets intended for senior citizens is the subject of this study. It seeks to thoroughly evaluate the efficiency of these wristbands in tracking physical activity and vital signs, evaluating their influence on health outcomes, and pointing out any potential drawbacks. The project uses an agile methodology to construct a unique Arduino device that uses sensors and IoT to monitor vital signs. It also integrates data analysis to identify the capacity of the device to response to user health issues. The device, named LifeGuardian, detects temperature and heart rate, giving important information about a person's general health. However, in the IoT, security and privacy for wearable devices are largely disregarded. It is essential to apply a systematic approach for security and privacy safeguards in the context of healthcare and remote health monitoring. This study adds knowledge on security and privacy of wearable smart health device of these IoT-enabled health bracelets for the elderly besides offers solutions for security and privacy.

I. INTRODUCTION

Inadequate health monitoring increases the likelihood of unanticipated health risks, which include unanticipated risks associated with undetected illnesses, postponed medical interventions, insufficient monitoring capacities, and a deficiency in health education [1]. Without routine monitoring, a number of health issues may go undiagnosed and have serious repercussions, including life-threatening events like heart attacks or abrupt cardiac arrests [1]. Utilizing the Internet of Things (IoT) and other rapidly developing technologies, smart health monitoring applications are made possible, allowing people to proactively monitor their health.

When it comes to IoT for medical device integration, the focus is shifted towards the consumer ends, such as Continuous Glucose Monitoring (SGM), blood pressure cuffs, ingestible sensors, connected inhalers and other devices designed to record data on patient vital signs however these wearable devices are lacking in terms of security and privacy which are paramount for patient safety of their personal health details and other related information's.

As many security breaches and data privacy issues are becoming common in medical sector [2] where these data collected over IoT devices are threatened by malwares and other interventions. Besides that, current state of IoT devices is also not adopting security measures which results concern on privacy data breaches and concern by user. Study by the Aruba research agency [3] states, IoT related security breaches exceeds 84% in 2019. As such, security measures should be investigated serious when adapting IoT related devices [4].

ISSN 2636-9680
eISSN 2682-9266

This study basically focuses on the development of smart health care for elderly users and how user acceptance towards lesser or no security measure IoT devices. Besides, this study also examines current states of security and privacy in terms of technical and challenges of implementing the health-related device.

The goal of this study is to develop an Internet of Things technology to create a health monitoring wristband which can improve personal health monitoring by elderly people however with no security measurements been taken into consideration and present the result on how user accept the devices besides discussing on the security measurement that should be included in any IoT device in near future.

II. RELATED WORK

Critical health issues are addressed by the LifeGuardian, which was created especially to meet the healthcare needs of senior citizens in an aging population that is at risk for heart disease [5]. An accelerometer, temperature sensor, heart rate sensor, emergency button, and other sensors are integrated into this user-friendly wearable to allow for continuous health monitoring and early health issue detection [6]. The goal of the gadget is to improve safety and offer immediate health insights, giving wearers access to real-time vital sign data so they can act quickly in an emergency. The addition of an emergency button, which makes calling for help simple, further guarantees wearer safety.

LifeGuardian and related products share fundamental ideas in the field of smart health bracelets. But to set itself apart, this initiative does extensive comparisons with the goal of developing a special and enhanced health monitoring gadget. The proposed bracelet emphasizes proactive health monitoring by aligning with IoT technological improvements, hence solving the shortcomings of traditional health monitoring methodologies outlined in the introduction.

TABLE 1: Differences between existing projects

Previous Project	Advantages	Disadvantages
MyBotic Durian UNO - Smart Patient Monitoring System [7]	Contains LCD display for displaying user health metrics.	Does not have an emergency button.
	Includes SpO2 sensor for blood oxygen level monitoring, including BPM monitoring.	Large.
	Includes LM35 Temperature Module, enabling body temperature tracking.	Lacks a battery to be fully portable and worn.
Pulse Oximeter! Measure Heart Rate and Oxygen Saturation using Max30102, Arduino and OLED Display [8]	Contains a similar LCD display to the MyBotic system.	Lacks temperature sensor.
	Tracks and measures BPM and SpO2 levels.	Push button can be seen as unnecessary and should've been used as an emergency button.
	Includes a push button that acts as a display navigator.	Unable to be worn, lack of a proper strap.
Heartbeat monitoring wrist band. Is it possible to make using MAX30102 module [9]	Comes with similar heartbeat sensing capabilities as other Arduino projects.	No SpO2 sensor for blood oxygen level monitoring.
	Smaller LCD display that project current wearer's readings.	Lack of an emergency button.

	Smallest size footprint amongst the bunch.	Similar to the other Arduino projects, with no distinguishing feature.

Table 1 shows that most of the project used similar items in the realm of Arduino projects, health monitoring systems have gained significant popularity. This is to provide a comparative analysis of three such Arduino projects: MyBotic Durian UNO, MountDynamics Health Monitoring System, and UT Go Health Monitoring Wristband. The analysis focuses on their advantages and disadvantages, enabling readers to make informed decisions when choosing a suitable health monitoring solution, whilst also giving the project team a foundation to base the initials ideas upon. However, based on the study, it revealed that no security measures have been included or taken into consideration.

Although the LifeGuardian's user-friendly design and continuous health monitoring features help older persons with important health problems [2], it is crucial to expand this attention to the security aspect. Strong security and privacy safeguards are required as IoT-enabled devices like LifeGuardian become more commonplace and potential vulnerabilities surface.

The significance of wearable device security is emphasized by research in the field of IoT security and privacy. It is crucial to guarantee the availability, confidentiality, and integrity of the data transferred and stored by health bracelets [4]. Big data collected from millions of IoT devices provide an impact on devices associated with medical care for data analytics. However, most security breaches and data privacy issues are reported in the medical sector [3]. For example, two Austrians meddled with the pain management infusion pumps and the overdose caused respiratory problems but could be fatal [10]. In another study, it is revealed that the FDA warned on pacemaker programmer models are at risk as outsiders can adjust the pacemaker setting in a patient through internet [10].

Therefore, it is imperative to adopt sufficient security measures to secure the medical systems, infrastructure, and protect the privacy of patient's sensitive personal data.

These studies highlight the necessity of adopting secure communication protocols and raising user knowledge of security and privacy in the context of wearable health monitoring devices to prevent data breaches and unwanted access to private health information [6]. To maintain user confidence and guarantee the safe and secure operation of these wearables, security elements must be incorporated into their design [7].

Another extensive survey conducted by Quadri et al. [1] that the security and privacy of IoT applications were overlooked, solutions prone to attacks and doesn't prescribe a robust security solution for healthcare IoT spectrum. It is also clear less research was carried out in the healthcare IoT in the past.

Strong security protections should be given top priority in the creation of the suggested health monitoring bracelet, which includes LifeGuardian, considering these observations. However, this security and privacy is what Lifeguardian failed to implement as well as much as many other studies on IoT in healthcare misses which impacted the need of using the device securely.

III. METHODOLOGY

The methodology that is used for the development of LifeGuardian is the Agile methodology as shown in **Fig 1**, which is an iterative and incremental approach to project development that prioritises adaptability, collaboration, and continuous improvement [11]. Unlike traditional waterfall methods, agile methodologies emphasise user collaboration, frequent feedback, and the delivery of working software in short development cycles called sprints. Agile projects are divided into phases, each with its specific objectives and deliverables.

ISSN 2636-9680
eISSN 2682-9266

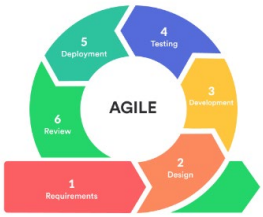

Fig. 1. Agile Methodology

This section explains the research methodology used and among others, on how the research data are being collected or generated. In addition, this section should also explain how the data collected are analyzed.

A. Requirements

The requirement phase serves as a crucial starting point for the project. The phase involves gathering essential knowledge to create a main framework of ideas for the LifeGuardian project. This phase is key to setting the stage of a successful development journey in revolutionizing the wearable devices that have emerged as valuable tools for monitoring and improving personal health.

B. Design

During the design phase, requirements are obtained and collected to begin creating an innovative health tracking bracelet. This phase also acts as the architectural stage, which follows a top-down technical approach. Various diagrams, such as the context circuit diagram, and flowchart, are used in this scenario to describe how the LifeGuardian bracelet would work, from receiving input to processing and providing the final output.

Fig 2 shows function circuit diagram is a simplified graphical representation of how different components in a circuit are connected. The diagram details the wiring and connections that are connected to create the circuit of the LifeGuardian bracelet.

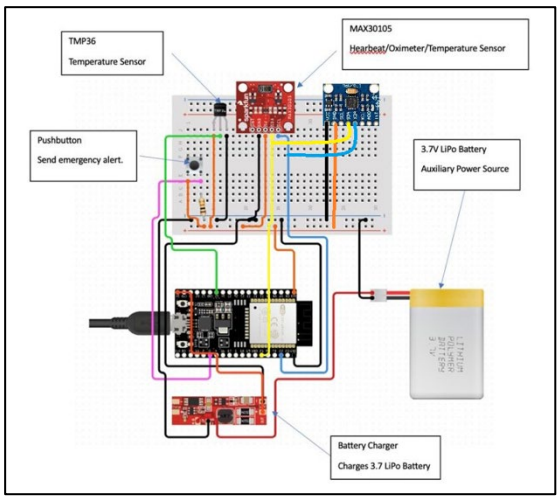

Fig. 2. Circuit Diagram

The ESP32 Arduino board acts as the main board that all sensors are connected to transmit data, whilst the main power source is from the 3.7 LiPo battery. After succesful connection, the ESP32 reads data from all sensors, and transmit the data to the Blynk API. Comparisons are done with the data readings to ensure theres no abnormalities, otherwise emergency alerts are sent to Blynk. Lastly, the health metrics data are displayed on connection mobile phones.

C. Development

After the design phase, the project is set to be developed. All planning, component specifications, and desired functionalities of the project are developed following increments for each separate functionality including the heart rate tracker, body temperature tracker, emergency button, impact and fall detection, mobile application synchronization, and notification functionalities. Development consists of creating the main code that interfaces with all components and synchronizes with a mobile phone for sensor readings to be interpreted and displayed. The LifeGuardian bracelet will be implemented feature by feature, tested to assure functionality, and then integrated and combined into a cohesive, fully functional wearable bracelet band.

D. Testing

The testing phase of LifeGuardian development is crucial for ensuring its accuracy, reliability, and performance in

measuring health data. This phase involves functional testing to validate the functionalities of the bracelet, including its sensors and features such as temperature, heartbeat, emergency button, and notifications. The high accuracy sensor of the Apple Watch provides readings like those of the LifeGuardian, while being significantly more expensive.

Performance testing is conducted to ensure the accuracy and dependability of these sensors, comparing their readings with calibrated devices of similar functions. Compatibility testing is also conducted to ensure the bracelet works seamlessly across end devices, uncovering any issues related to data synchronization, connectivity, or performance. Thorough testing is done to identify and uncover future issues that may arise and take pre-active actions to eliminate further anomalies which guarantee precise and trustworthy data. However, security and privacy has been ignored which is a serious measure that must be avoided by any cost during IoT devices development process especially on health care monitoring.

E. Deployment

The deployment phase of the project follows an iterative approach. Iterative deployment involves small, frequent releases based on user feedback and priorities. User acceptance testing validated integration and deployment, with feedback driving further improvements. Deployment procedures assisted in completing the process, and continuous monitoring provided real-time data for ongoing enhancements. Through Agile methodology, LifeGuardian achieved seamless integration and deployment into successfully creating and delivering a high-quality bracelet that tracks the wearers health metrics and provides a warning system for guardians.

F. Review

The primary objective of the review phase is to assess the implemented features, identify any gaps or discrepancies, and validate their alignment with the project's requirements. During review meetings, the team presents the completed work, demonstrating the functionality and usability of the LifeGuardian. Feedback and suggestions from the target scope are gathered, and necessary adjustments or improvements are noted for implementation in subsequent sprints.

IV. RESULTS AND ANALYSIS

Fig 3 shows the main dashboard that displays the current health metrics of the wearer. The wearer's heart rate (BPM), and body temperature (Celcius) are displayed as a gauge for the current readings, in addition to a chart that shows the patterns of the readings.

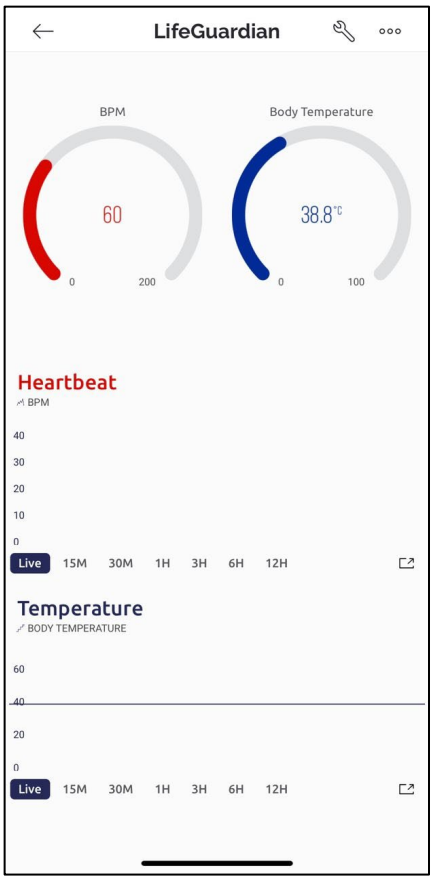

Fig. 3. Main Dashboard

Summarize the findings in text and illustrate them. Where appropriate, use figures and tables. In text, describe each of the results, pointing the reader to observations that are most relevant to the problem. Analyze the data and prepare the analyzed (converted) data in the form of figures (graph), table, or in text form.

Fig 4 showcases when the emergency button on the wearer's bracelet is pressed, a notification is triggered and sent to the Blynk API. This

ISSN 2636-9680
eISSN 2682-9266

notification act as an alert, indicating that the wearer is in danger or requires immediate assistance. The Blynk API shows this notification by sending the emergency alert to wearer close contact and triggering predefined actions, ensuring a prompt response to the wearer's emergency.

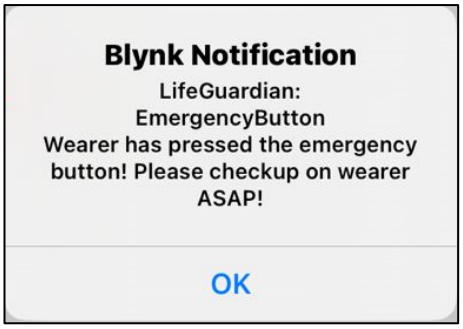

Fig. 4. Emergency Alert

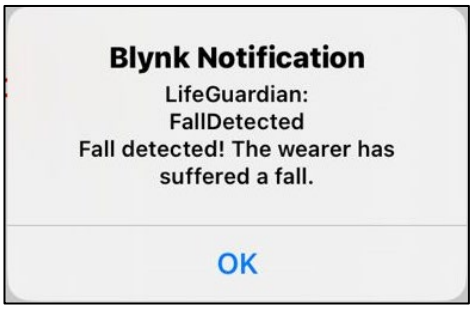

Fig. 5. Fall Detection Alert

While **Fig 5** showcases when the wearer experiences a fall, the sensor triggers a notification within the Blynk system. This notification act as an alert to inform the wearer close contact about the incident. By leveraging the sensor's capabilities, the Blynk API ensures prompt detection of falls and facilitates immediate communication to ensure the wearer's safety.

From the development process, it is clearly shown that no security nor privacy was included in any phases of the methodology. This might result in the acceptance of such devices as user are concern on their personal health information is on the internet and easily can be share or misused if these security measure are not conformed into the device and during development process.

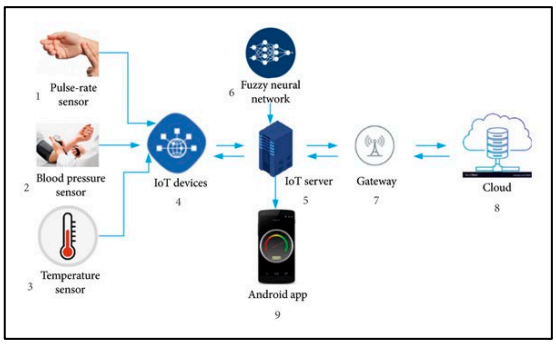

Fig. 8. Smart health Architecture

Wearables and sensors Healthcare devices use WiFi, Bluetooth, and Zigbee to transmit medical data to a gateway via cloud services and edge or node computing. The processing layer of wide-area communication technologies like 4G LTE, LoRaWAN, and NB-IoT subsequently carries this farther to the data center. The data center processes and analyzes this massive volume of data before sharing specific information with each patient [12].

The major challenge in implementing security measures for IoT in healthcare is the devices that enter through various channels to the network systems. Open WiFi or personal hotspots networks are used to connect a huge number of diverse devices—without encryption or passwords—to the internet. Hackers may target specific people to disable their device and prevent access to life-saving care, begin a general attack on a specific type of device, or steal data. According to [12], the key security measure must be considered in IoT for healthcare is that data confidentiality, integrity, authentication, and authorization besides adapating ISO security and privacy standards ISO 25237:2017 in which standard provides various techniques including pseudo randomization to anonymize the data in the health domain. Adapting the standards allows the patients to trust in e-Healthcare enterprises while also allowing for healthcare record sharing for research without compromising privacy.

V. DISCUSSION

As such in this development study, potential improvements may include the integration of additional health metrics, such as oxygen saturation or stress levels, or the exploration of advanced machine learning techniques to provide personalized health insights. The device does not complete the evaluation on public as its concern on security and privacy that was failed to be adapted as the study does not want to collect any personal data without knowing the consequences it can bring to the user.

Machine learning (ML), deep learning (DL), blockchain, or nanotechnologies, and fog computing are a few of the novel solutions that could fill the gaps and enhance the existing security architecture of IoT of healthcare devices [12].

By envisioning and discussing these future improvements, the project group aims to lay the groundwork for continuous innovation, ensuring that the LifeGuardian remains at the forefront of innovating the health monitoring technology and continues to make a positive impact on the lives of individuals susceptible to heart disease.

VI. CONCLUSION

In conclusion, the objective to develop a health product that uses the IoT concept was achieved by producing a new model of wearable device which can give many benefits for people to keep track of their health. Through the testing, this project was proven to reach the expected outcome which fulfilled the objective of this project. The devices must be added security and privacy measurement before being tested for its accuracy or other variables that might produce good result for future use and benefits many especially the healthcare system. However a deep review on past studies regarding this security and privacy to support the need of such devices and user acceptance.

VII. ACKNOWLEDGEMENT

The authors would also like to thank the Centre for Diploma Studies, Universiti Tun Hussein Onn Malaysia for its support.

VIII. REFERENCES

[1] M. A. Martínez-González, A. Gea, and M. Ruiz-Canela, “The Mediterranean Diet and Cardiovascular Health,” Circulation Research, vol. 124, no. 5, pp. 779–798, Mar. 2019, doi: 10.1161/circresaha.118.313348.

[2] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies,” IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020

[3] Aruba Networks, “IoT Heading for Mass Adoption by 2019 Driven by Better-Than-Expected Business Results,” arubanetworks.com, 2017. [Online]. Available: https://news.arubanetworks.com/press-release/arubanetworks/iotheading-mass-adoption-2019-driven-better-expected-businessresults. [Accessed: 28-Jul-2020]

[4] P. A. H. Williams and V. McCauley, “Always connected: The security challenges of the healthcare Internet of Things,” in 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, 2017, pp. 30–35

[5] Larnyo, E.; Dai, B.; Larnyo, A.; Nutakor, J.A.; Ampon-Wireko, S.; Nkrumah, E.N.K.; Appiah, R. Impact of Actual Use Behavior of Healthcare Wearable Devices on Quality of Life: A Cross-Sectional Survey of People with Dementia and Their Caregivers in Ghana. Healthcare 2022, 10, 275.

[6] D. Martinho, J. Carneiro, J. M. Corchado, and G. Marreiros, “A systematic review of gamification techniques applied to elderly care,” Artificial Intelligence Review, vol. 53, no. 7, pp. 4863–4901, Feb. 2020, doi: 10.1007/s10462-020-09809-6.

[7] Arduino IOT Smart Patient Monitoring system with BLYNK Durian UNO (Enhancement Of Arduino UNO),” Arduino IOT Smart Patient Monitoring system with BLYNK Durian UNO (Enhancement Of Arduino UNO). https://mybotic.com.my/arduino-iot-smart-patient-monitoring-system-with-blynk-durian-uno-enhancement-of-arduino-uno

[8] “Pulse Oximeter! Measure Heart Rate and Oxygen Saturation using Max30102, Arduino and Oled Display,” YouTube, Jun.

ISSN 2636-9680
eISSN 2682-9266

14, 2021. https://www.youtube.com/watch?v=W_3ljVlt7Sk

[9] "Heart beat monitoring wrist band. Is it possible to make using MAX30102 module ? | Ut Go," YouTube, May 12, 2020. https://www.youtube.com/watch?v=qI_456UPf5Y

[10] FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," FDA Guid., p. 6, 2018.

[11] V. Venkatesh, J. Y. L. Thong, F. K. Y. Chan, H. Hoehle, and K. Spohrer, "How agile software development methods reduce work exhaustion: Insights on role perceptions and organizational skills," Information Systems Journal, vol. 30, no. 4, pp. 733–761, Mar. 2020, doi: 10.1111/isj.12282.

[12] Karunarathne, Sivanarayani M., Neetesh Saxena, and Muhammad Khurram Khan. "Security and privacy in IoT smart healthcare." *IEEE Internet Computing* 25.4 (2021): 37-48.

OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
43 - 52

Enhancing An Iris Detection Using Integration of Semantic Segmentation Architecture and Data Augmentation

Warusia Yassin[1], Mohd Faizal Abdollah[1], Sasikumar Gurumoorthy[2], Kumar Raja[3] and Izzatul Nizar[1]
[1]Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[2]J.J. College of Engineering and Technology, Trichy, India
[3]REVA University, Bengaluru, India

ARTICLE INFO

Article History
Received 3 Jun 2024
Received in revised form 29 Jun 2024
Accepted 1 Jul 2024

Keywords: Iris Recognition, Data Segmentation, Data Augmentation, Mask R-CNN, Accuracy

ABSTRACT

An iris recognition is a biometric way of identifying people in the ring-shaped portion of the eyeball surrounding the pupil. An iris recognition is used in biometrics because each iris is unique to an individual. Unfortunately, even though researchers have considered various approaches to improve the detection of iris recognition, obtaining higher accuracy remains a challenging task. More specifically, the major drawbacks contributed by the poor quality of images such as blur, lighting infection, and data scarcity. Therefore, in this work, we proposed the utilization of semantic segmentation and data augmentation approach to enhance the iris detection capability in terms of accuracy. The semantic segmentation (SS), a part of Mask R-CNN, is applied to overcome the image quality limitation. This approach partitions an image into multiple image segments known as image regions to differentiate dissimilar objects in an image using pixel level. Subsequently, using the data augmentation (DA) approach, new data is derived artificially from existing data that has been effective in improving the model generalization and precisely solving issues of data scarcity. The proposed model namely SS+DA has been evaluated using benchmark datasets known as CASIA and IITD. The experiment result shows that the proposed method is able to obtain an above 99% accuracy rate for both the CASIA and IITD datasets.

I. INTRODUCTION

Conventional methods of human identification, such as keys, passwords, and access cards, have given a means of identifying biological patterns such as the face, voice, fingerprint, iris, and finger vein. Face, voice, fingerprint, iris, and finger vein patterns are all frequently employed for personal identification. Existing research [1], [2] has demonstrated that, of the aforementioned biological patterns, the iris pattern is the most reliable and secure form of personal identification due to significant advantages such as stability, informativeness, safety, contact lessness, and many more. Considering these benefits, iris recognition has increased in popularity as well, and many studies from diverse researchers continue to focus on iris identification [3], [4].

Deep learning-based algorithms, notably ones based on various Convolutional Neural Network designs, have led to significant improvements in many computer vision applications over the previous decade. It's not unforeseen that, in terms of biometrics technology, iris recognition has seen a surge in the use of solely data-driven approaches at all stages of the recognition pipeline, from preprocessing (such as off-axis gaze correction), segmentation, and encoding to matching. However, the impact of deep learning on different phases of the iris identification pipeline is unequal [5], [6].

Unfortunately, iris recognition is regarded as an impenetrable topic, with most results indicating space for improvement. For many years, this issue has motivated various research

ISSN 2636-9680
eISSN 2682-9266

projects. Despite the clear improvement in the effectiveness of such techniques, they all confront unique challenges when dealing with severely degraded data. Images are commonly blurred in motion, poorly focused, partially obscured, and off-angle. Furthermore, in the case of visible light data, strong reflections from the environments surrounding the people are readily apparent further complicating the segmentation task.

Hence, in this work, we propose modified semantic segmentation and integration of data augmentation to enhance the detection performance of iris recognition in terms of accuracy. Semantic segmentation (SS), an element of Mask R-CNN, is employed to overcome the quality of image constraints. This method divides an image into many picture segments known as image regions to distinguish various items in an image at the pixel level. Following that, new data is produced artificially from existing data using the data augmentation (DA) strategy, which has been effective in increasing model generalization and accurately fixing data scarcity challenges.
The remainder of the part is structured as follows: Section 2 comprises the discussion of the related work in which several similar previous studies have been explored and reviewed. The overall detail of the proposed methods has been briefly explained in Section 3. Section 4 discusses the obtained result via conducted experiments using different benchmark datasets and is followed up by the summary and future work in Section 5.

II. RELATED WORK

Identity authentication has advanced its methods by utilizing iris biometrics [7] rather than fingerprints and other physical identity authentication technologies. Iris biometric authentication [8] gradually increased stability beyond the age of three due to uniqueness, random patterns with higher complexity, a highly protected interior eye, and feature stability. Iris biometric systems extract the iris to obtain ocular information to identify individuals, hence iris localization is critical. These applications in several sectors emphasize the relevance of pupil localization in diagnosing diseases, enforcing safety, and enforcing security, among other things. As a result, eye-tracking installations are required in these circumstances [9].

Deep learning has transformed iris identification, a biometric tool utilized to recognize people based on the distinctive patterns found on their iris. Conventional approaches were based on handcrafted features and algorithms, but deep learning techniques, notably convolutional neural networks (CNNs), have significantly increased accuracy and efficiency. Iris detection with deep learning often involves preprocessing the picture of the iris to improve contrast and reduce noise. Next, the model of CNN is used for extracting characteristics from the iris patterns. These attributes are learned via training on a huge dataset of iris images. Throughout the training procedure, CNN is learning to recognize subtle patterns in the iris, including furrows, crypts, and freckles that are distinctive for every person. The algorithm repeatedly adjusts its parameters via backpropagation, reducing the disparity between anticipated and actual iris properties. After training, the deep learning algorithm can correctly recognize humans through comparing current iris scans to previously established patterns. This procedure, known as iris matching, compares the similarities of iris characteristics retrieved from an input image with those preserved in a database. In general, deep learning has considerably increased the accuracy as well as the dependability of iris identification systems, rendering them useful for a variety of purposes particularly identity verification [6], [10].

The segmentation of the iris is a critical stage in iris recognition. Feeding a segmented iris image into a recognition approach often yields better results than utilizing the whole iris image. Traditional manual iris segmentation methods are computationally complex and necessitate substantial specialist knowledge. Numerous investigations have focused on segmenting iris images employing deep learning approaches to accomplish iris segmentation more conveniently and reliably. Unfortunately, the detection of iris is seen as an extremely challenging problem that indirectly has motivated numerous research works for decades in achieving higher performance in iris recognition. Regardless of the clear

improvement in the effectiveness of such techniques, they all confront unique challenges when dealing with severely degraded data. Images are regularly blurred by motion, are poorly focused, are partially occluded, and are off angle. Furthermore, harsh reflections from the environs surrounding the people are visible in the context of light-sensitive data, adding to the difficulty of the segmentation process [3], [11], [12]

Recently, consisting of many other computer vision problems, DL-based architectures have been claimed as giving consistent progress above the state-of-the-art for the iris segmentation difficulty, with various models presented. Table 1 provides a unified view of the most essential current DL-based methodologies, with the approaches listed in chronological order.

TABLE 1: Previous Study in Iris Recognition

Author/Year	Methods	Data	Objective	Result
[13]	Deep Semantic Segementation	CASIAv4 IITD	Proposing deep semantic segmentation in improving performance such as accuracy	CASIA (98.51%) IITD (98.4%)
[14]	CNN, VGG16, ResNet, Inception	Custom Dataset	Proposing a reliable method for detecting corneal arcus with high accuracy	ResNet (88%) Inception (77%) VGG16 (72%)
[15]	CNN, VGG19, ResNet	UBIPr Database	Proposing novel method in improving accuracy using periocular territory	VGG19 (96%) ResNet18 (88%)
[16]	CNN, VGG16, ResNet50, Inception, v3	CASIA UBIRISv2	Proposing a DCNN model to identify dissimilar photos that able to improve the accuracy	CASIA (99.64%) UBIRIS (98.76%)
[17]	CNN	CASIA UBIRISv2	Improving segmentation of iris pictures to obtain higher accuracy	CASIA (99.5%) UBIRISv2 (98.92%)
[18]	Deep CNN, DenseNet	ND Database IIITD Database	Proposing a novel DCLNet to obtain higher accuracy	IITTD (99.10%) ND (84.34%)
[19]	DNN	CASIA UBIRISv2	Combine DNN with an augmentation strategy to increase the quality of poor photos	CASIA (99.71%) UBIRISv2 (97.82%)
[20]	CNN Encoder_decoder Network Semantic Segmentation	CASIAv4 IITD UBIRISv2	Proposing fully residual encoder and decoder network for accurate iris segmentation	CASIAv4 (96.59%) IITD (96.82%) UBIRISv2 (94.31%)

Several explorations and experiments have been conducted by the research community to improve iris recognition as illustrated in Table 1. Diverse methods and approaches have been taken into consideration to improve iris recognition via different strategies by employing augmentation, segmentation, CNN, and so forth. For instance, [13] have proposed a dual-path fusion network model by integrating deep semantic segmentation that strengthens the ability to extract significant features in contrast to the conventional approaches. Furthermore, using this method, to enhance the segmentation accuracy, parallel branches are constructed to extract shallow spatial features into the main network and merge shallower spatial information alongside deep semantic information. The proposed methods have been evaluated against well-known CASIA and IITD benchmark datasets and managed to obtain 98.5% and 98.4% accuracy rates respectively.

ISSN 2636-9680
eISSN 2682-9266

Furthermore, [14] created a dependable approach and technology for detecting the presence of Corneal Arcus (CA). The approach can automatically detect the existence of CA in patients with undiagnosed Familial Hypercholesterolemia (FH), which was previously hard to determine. The authors stated that utilizing CNN, VGG16, Resnet, and Inception algorithms resulted in high accuracy scores and a great association with expert decisions.

[15] attempted to tackle the iris recognition systems that were presented with non-ideal photos that caused poor performance. To address the problem, the authors evaluate the usability of the periocular region, a new feature-rich biometric trait, in two non-ideal scenarios: picture matching with different position variations and image matching on different sides of the periocular. The authors claimed that VGG19 has 94% and 96% accuracy for photos with 30 and -30 degree posture variation, respectively, and Resnet18 has around 88% for matching images on the same side.

Additionally, a study by [16] em
ployed pre-trained DCNN models to connect images from the same subject and detect dissimilar shots from different subjects to explore more distinguishing traits from the periocular region or iris. The authors solved the problem of images suffering from various noise artifacts such as shadows, specular reflections, occlusion by the eyelid, eyelashes, hair, off-angle, motion-blur, and rotational as a result of carrying imaging conditions, resulting in data inadequacy and complicating the recognition task by using VGG16, Resnet50, and Inception-v3.

In addition, [17] aim to improve the segmentation of off-axis iris images taken by a user-facing camera in uncontrolled settings on a wearable AR/VR device. Frontal iris region segmentation is compared to state-of-the-art algorithms with substantially higher complexity to achieve excellent levels of performance. The authors tackled the problem of near-eye iris segmentation, a new challenge brought on by the emergence of growing AR/VR headset technology. Although the dataset of iris samples captured from a user-facing camera on AR/VR devices is a significant barrier, the authors stated that the results show promising levels of off-axis segmentation accuracy, and the resulting trained neural network significantly outperforms state-of-the-art frontal iris segmentation.

[18] also claimed that, despite significant improvements in iris identification, contact lenses might be considerably deceiving as the contact lens folds all around the iris region difficult to be collected. Consequently, the authors present a novel Densely Connected Contact Lens Detection Network (DCLNet), known to be a deep convolutional network with dense connections between layers. DCLNet was constructed by modifying DenseNet121 and then adding a Support Vector Machine (SVM) classifier.

However, in an effort to address the issue where acquisition becomes less constrained and the quality of images is frequently worse than concentrated iris acquisition methods, [19] also make an effort at introducing an end-to-end deep neural network model with an augmentation strategy that significantly enhances the quality of iris segmentation on less high-quality photos. The authors use Fully Convolutional Deep Neural Network (FCDNN) and Semi Parallel Deep Neural Network (SPDNN) to tackle the difficulties.

On the other hand, non-ideal conditions caused by external light and sound, along with user non-cooperation, that affect iris performance, are resolved by [20] utilizing Semantic Segmentation, CNN, and Encoder-Decoder Network. The exploratory outcomes showed that the suggested approach functioned as best it could, according to the authors. While this was going on,

Based on prior research in similar disciplines, gaps in poor-quality photos, such as blur and poor illumination, caused the method to fail to recognize iris images more correctly. Therefore, the detection precision of the method is low, and the images contain numerous noise artifacts such as shadows, reflections, occlusion by the eyelashes and eyelids, or off-angle, which hinder the recognition process owing to diverse imaging conditions. Therefore, an innovative approach

is necessary to bridge the aforementioned gaps, which have become a difficult task to complete nowadays. Consequently, the objective of this research has focused on proposing the enhancement of semantic segmentation and data augmentation to improve detection performance in terms of accuracy, specifically for blur and poor lighting-infected images.

III. PROPOSED SOLUTION

The proposed solution includes a modified Semantic Segmentation structure which is adopted with a Data Augmentation module. Figure 1 illustrates the architecture of the proposed solution namely MSSDA (Modified Semantic Segmentation Data Augmentation) which enables iris recognition more accurately.

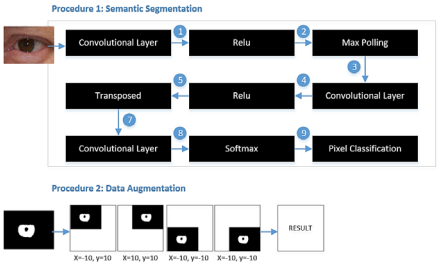

Fig. 1. The overall architecture of the proposed MSSDA

The employed Semantic Segmentation is a part of Mask R-CNN that can generate the mask and pixel label. Furthermore, object detection is distinct from Semantic segmentation, yet it constructs the mask for the considered object. Semantic segmentation took on the task of separating pixels and determining which pixels belong to which object or class. Referring to Figure 1, the overall MSSDA comprises several sequential layers i.e. Input, Convolutional, Max Pooling, RELU, Transposed, Softmax, and Pixel Classification. In particular, two strategies will be used in the implementation procedure: semantic segmentation and data augmentation. The main aim of utilizing semantic segmentation is to produce mask and pixel labels for image classification that can facilitate object detection more accurately.

Semantic segmentation will divide a picture into several segments, or regions, every single one which is associated with a particular class or category. In addition, this semantic segmentation provides a comprehensive comprehension of an image's information by assigning an identity to each pixel, in contrast to simple object recognition, which aims to identify and locate things within an image. Convolutional layers are the first layer we utilized since they are important for extracting characteristics from input images, which the created network uses to classify every pixel into meaningful segments. To enable the network to identify specific characteristics from the input image, such as edges, corners, object classes, categories, and so on, the extracted hierarchical features will be in various levels of abstraction. Max pooling layers are taken into consideration when the non-linear activation function known as RELU (Rectified Linear Unit) is used to lower the special dimensions of the feature map, translation invariance, and computational effectiveness. More specifically, the RELU activation function is utilized to add non-linearity to the formed network for a deep understanding of the complex relationship between input features and output labels. More specifically, for deep networks, this straightforward technique helps the network understand more quickly and avoids the issue of vanishing gradients, which can arise during training if the gradient gets smaller than necessary.

Subsequently, the generated feature maps' spatial dimension was reduced progressively using the max polling function, which indirectly improved the effectiveness of the semantic segmentation model. Moreover, by expanding the network's receptive field, max pooling enables neurons in lower layers to gather data from a larger region of the supplied image. For precise semantic segmentation, this helps the network understand deeper features and context.

Transposed convolution layers are included inside the network to improve the feature maps' spatial resolution. By first executing a convolution process using learnable parameters, and then expanding the zeros using a stride-based method, the implemented transposed convolution efficiently "upsamples" the feature maps, producing an expanded feature map. This has facilitated the precise and more accurate pixel-wise segmentation masks with fine details.

ISSN 2636-9680
eISSN 2682-9266

The softmax function is employed before the final phase of the network in semantic segmentation to generate pixel-wise class probabilities for every pixel in the image being analyzed. The resultant feature map is subjected to the softmax function, which transforms the raw scores into probabilities for each of the pixels that add up to one for all classes. Each pixel's expected probability distribution for each class is represented by the softmax function's output. During inference, the class with the highest probability is often selected as the predicted class for each pixel. Finally, in this procedure, the pixel classification assigned class labels for the entire processed images individually with the aim of the detailed information about the context of the images can be obtained.

On the other side, later the augmentation approach is considered to reduce the overfitting within images, as the performance of the accuracy has tendencies for improvement. Upon receiving the output from prior procedure, the pixel data and image data combined respectively to facilitate training time to obtained desired accuracy. The translation approach has been applied in which each iris image is shifted horizontally and vertically to simulate changes in position of -10 or +10 randomly at x-axis and y-axis within its bounding box. This modification represents alterations to the orientation of the iris around the eye, making the model more reliable in real-world circumstances. By performing translation modification to iris photos, the augmented dataset becomes greater in variety, accounting for differences in iris orientation that could happen in real-world circumstances. This improves the resilience and generalizability of the proposed model for iris detection, resulting in greater performance in real applications.

IV. EXPERIMENTS & RESULT

Dataset

The CASIA v4 Interval and IITD benchmark datasets have been utilized for assessing the suggested method. CASIA Iris Image Database (CASIA-Iris) was created by the Center for Biometrics and Security Research (CBSR) research team and is now available to the international biometrics community. CASIAv4 Interval, in particular, offers a collection of images captured using their close-up iris camera. The most enticing aspect of the iris camera is the circular NIR LED array with appropriate luminous flux for the iris. CASIAv4 Interval is perfect for studying iris image fine texture properties. The IITD collection known as the IIT Delhi Iris Database, on the other hand, principally consists of iris photographs taken from IIT Delhi students and staff. It is accessible for free upon request, and the photographs are saved in bitmap format. The subjects in the database range in age from 14 to 55, with 176 men and 48 women. In this research, the CASIAv4 Interval database comprises 2446 samples from 142 subjects, whereas the IITD database contains 2240 picture samples from 224 subjects. The whole set of iris images from the right eye was used as a training set, whereas the first five photographs from the left eye were used as a test set. As a result, the test set contains 2240 authentic pairs and 624,400 counterfeit pairs.

Evaluation Measurement

The proposed method's performance was evaluated by calculating the accuracy. These metrics are commonly used to assess the performance of some recognition systems (Prathaban, B.P., and Balasubramanian, R. (2020, December 24). The employed formula is as follows:

$Accuracy = (TP + TN) / (TP + FP + TN + FN)$

FP = False Positive number of imposter acceptance.
TN = True Negative number of imposter rejection
FN = False Negative number of genuine rejection
TP = True Positive number of genuine acceptance.

CASIA Iris Image Database (CASIA-Iris) was created by the Center for Biometrics and Security Research (CBSR) research team and is now available to the international biometrics community. CASIAv4 Interval, in particular, offers a collection of images captured using their close-up iris camera. The most enticing

aspect of the iris camera is the circular NIR LED array with appropriate luminous flux for the iris. CASIAv4 Interval is perfect for studying iris image fine texture properties. The IITD collection known as the IIT Delhi Iris Database, on the other hand, principally consists of iris photographs taken from IIT Delhi students and staff. It is accessible for free upon request, and the photographs are saved in bitmap format. The subjects in the database range in age from 14 to 55, with 176 men and 48 women.

Experimental Result

A set of experiments were carried out to assess the effectiveness of the proposed method. Initially, the labeled data (specifically, pixel label data) will be blended with the image or original data during the semantic segmentation phase. This is due to the data augmentation phases being processed utilizing a variety of epochs such as 10, 20, and 30. Table 2 represents the output from the training stages for two different datasets.

TABLE 2: Training Result

Dataset	Epoch	Accuracy (%)
CASIAv4	10	96.01
	20	99.41
	30	99.99
IITD	10	99.18
	20	99.9
	30	99.94

Based on the obtained results in Table 2, epochs influence determining the success of the suggested strategy during the training stage. The greater the number of epochs, the greater the accuracy. This is because when the epochs increase, the image is divided into a small partition, making it clearer and, as a result, increasing the accuracy of the suggested method. For instance, the obtained result via CASIAv4 and IITD dataset of epochs 30 are slightly higher in terms of accuracy at 99.9% as compared to other epochs.

TABLE 3: Previous State-of-the-art Methods Vs Proposed Method

Dataset	Author	Approach Used	Accuracy
CASIAv4	[21]	Iris Segmentation	91.86%
	[20]	CNN, Semantic and Segmentation	96.59%
	[22]	CNN	99.24%
	[13]	Deep Semantic Segmentation	98.51%
	The Proposed Method	*Semantic Segmentation + Data Augmentation*	*99.9%*
IITD	[23]	Mask R-CNN	96%
	[20]	CNN, Semantic and Segmentation	96.82%
	[24]	Deep CNN, Semantic and Segmentation	94.08%
	[13]	Deep Semantic Segmentation	98.40%
	The Proposed Method	*Semantic Segmentation + Data Augmentation*	*99.94%*

Furthermore, as shown in Table 3, previous work that employed deep learning as a foundation, similar techniques, and well-known datasets such as CASIAv4 and IITD have been compared to the proposed method. The proposed method has outperformed the entire previous work in terms of accuracy. Referring to Table 3, the proposed method has achieved a 99.9% accuracy rate for both CASIAv4 and IITD datasets. The work proposed by Shalaby et al (2021) gained 99.24% via the CASIAv4 dataset and via the TTDI dataset and it is the closest state-of-the-artwork that is slightly gained near to the proposed method. Additional analysis is being performed of the results collected to discover potential improvements. A brief tracing is carried out utilizing the model's output for detection and the label of the data. Unfortunately, because of the image not being

ISSN 2636-9680
eISSN 2682-9266

appropriately labeled, the identical generated pattern makes recognizing the other region difficult. As a result, even though the image is quite clear, the pixel labels could not be made precisely. To achieve a better result, an improved approach to image enhancement should be implemented. However, a concentrated examination of image tagging on unconstrained images is required.

V. CONCLUSION AND FUTURE WORK

The proposed method comprises an integrated component of Semantic Segmentation and Data Augmentation, namely SSDA. This method breaks an image into numerous picture portions known as image regions to distinguish between dissimilar objects from an image at the pixel levels. Furthermore, using the data augmentation (DA) strategy, novel information is artificially produced from current data, which has proven useful in increasing model generalization and accurately resolving data scarcity issues. The suggested model, SS+DA, has been tested on benchmark datasets known as CASIA and IITD. The experiment results reveal that the proposed strategy achieves an accuracy rate of more than 99% for both the CASIA and IITD datasets. For future work, the research under iris recognition could be suggested to incorporate data augmentation methods with dissimilar approaches and validate using real-time data.

VI. ACKNOWLEDGEMENT

The authors would like to appreciate the university Universiti Teknikal Malaysia Melaka and the industry ASK-Pentest Sdn Bhd for their funding and encouragement.

VII. REFERENCES

[1] M. Mostofa, S. Mohamadi, J. Dawson, and N. M. Nasrabadi, "Deep GAN-Based Cross-Spectral Cross-Resolution Iris Recognition," IEEE Trans Biom Behav Identity Sci, vol. 3, no. 4, pp. 443–463, 2021, doi: 10.1109/TBIOM.2021.3102736.

[2] A. S. Al-Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi, and T. A. M. Nagem, "A multi-biometric iris recognition system based on a deep learning approach," Pattern Analysis and Applications, vol. 21, no. 3, pp. 783–802, 2018, doi: 10.1007/s10044-017-0656-1.

[3] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst Appl*, vol. 143, p. 113114, 2020, doi: 10.1016/j.eswa.2019.113114.

[4] J. Sun, S. Zhao, S. Miao, X. Wang, and Y. Yu, "Open-set iris recognition based on deep learning," *IET Image Process*, vol. 16, no. 9, pp. 2361–2372, 2022, doi: 10.1049/ipr2.12493.

[5] F. Alonso-Fernandez, K. Hernandez-Diaz, S. Ramis, F. J. Perales, and J. Bigun, "Facial masks and soft-biometrics: Leveraging face recognition CNNs for age and gender prediction on mobile ocular images," *IET Biom*, vol. 10, no. 5, pp. 562–580, 2021, doi: 10.1049/bme2.12046.

[6] Y. Yin, S. He, and R. Zhang, "Deep Learning for Iris Recognition : A Review arXiv : 2303 . 08514v1 [cs . CV] 15 Mar 2023 Deep Learning for Iris Recognition : A Review," *Springer Nature*, no. September, 2023.

[7] W. Zhou, X. Lu, and Y. Wang, "A Robust Pupil Localization via a Novel Parameter Optimization Strategy," *Wirel Commun Mob Comput*, vol. 2022, p. 2378911, 2022, doi: 10.1155/2022/2378911.

[8] F. Jan and N. Min-Allah, "An effective iris segmentation scheme for noisy images," *Biocybern Biomed Eng*, vol. 40, no. 3, pp. 1064–1080, 2020, doi: 10.1016/j.bbe.2020.06.002.

[9] R. Rathnayake *et al.*, "Current Trends in Human Pupil Localization: A Review," *IEEE Access*, vol. 11, no. October, pp. 115836–115853, 2023, doi: 10.1109/ACCESS.2023.3325293.

[10] K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep Learning for Iris Recognition: A Survey," vol. 1, no. 1, pp. 1–35, 2022, [Online]. Available: http://arxiv.org/abs/2210.05866

[11] A. Kintonova, I. Povkhan, M. Mussaif, and G. Gabdreshov, "Improvement of Iris Recognition Technology for Biometric Identification of a Person," *Eastern-European Journal of Enterprise Technologies*, vol. 6, no. 2–120, pp. 60–69, 2022, doi: 10.15587/1729-4061.2022.269948.

[12] S. Jamaludin *et al.*, "Advances in Engineering Software Efficient , accurate and fast pupil segmentation for pupillary boundary in iris recognition," *Advances in*

Engineering Software, vol. 175, no. October 2022, p. 103352, 2023, doi: 10.1016/j.advengsoft.2022.103352.

[13] S. Lei, A. Shan, B. Liu, Y. Zhao, and W. Xiang, "Lightweight and efficient dual-path fusion network for iris segmentation," Sci Rep, vol. 13, no. 1, pp. 1–13, 2023, doi: 10.1038/s41598-023-39743-w.

[14] T. Kocejko, J. Ruminski, M. Mazur-Milecka, M. Romanowska-Kocejko, K. Chlebus, and K. H. Jo, "Using convolutional neural networks for corneal arcus detection towards familial hypercholesterolemia screening," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 7225–7235, 2022, doi: 10.1016/j.jksuci.2021.09.001.

[15] P. Kumari and K. R. Seeja, "Periocular Biometrics for non-ideal images: With off-the-shelf Deep CNN & Transfer Learning approach," Procedia Comput Sci, vol. 167, no. 2019, pp. 344–352, 2020, doi: 10.1016/j.procs.2020.03.234.

[16] S. Umer, A. Sardar, B. C. Dhara, R. K. Rout, and H. M. Pandey, "Person identification using fusion of iris and periocular deep features," Neural Networks, vol. 122, pp. 407–419, 2020, doi: 10.1016/j.neunet.2019.11.009.

[17] V. Varkarakis, S. Bazrafkan, and P. Corcoran, "Deep neural network and data augmentation methodology for off-axis iris segmentation in wearable headsets," *Neural Networks*, vol. 121, pp. 101–121, 2020, doi: 10.1016/j.neunet.2019.07.020.

[18] M. Choudhary, V. Tiwari, and U. Venkanna, "An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM," *Future Generation Computer Systems*, vol. 101, pp. 1259–1270, 2019, doi: 10.1016/j.future.2019.07.003.

[19] S. Bazrafkan, S. Thavalengal, and P. Corcoran, "An end to end Deep Neural Network for iris segmentation in unconstrained scenarios," *Neural Networks*, vol. 106, pp. 79–95, 2018, doi: 10.1016/j.neunet.2018.06.011.

[20] M. Arsalan, D. S. Kim, M. B. Lee, M. Owais, and K. R. Park, "FRED-Net: Fully residual encoder–decoder network for accurate iris segmentation," *Expert Syst Appl*, vol. 122, pp. 217–241, 2019, doi: 10.1016/j.eswa.2019.01.010.

[21] A. Gangwar, A. Joshi, A. Singh, F. Alonso-Fernandez, and J. Bigun, "IrisSeg: A fast and robust iris segmentation framework for non-ideal iris images," 2016 International Conference on Biometrics, ICB 2016, 2016, doi: 10.1109/ICB.2016.7550096.

[22] A. S. Shalaby, R. Gad, E. E.-D. Hemdan, and N. El-Fishawy, "An efficient CNN based encrypted Iris recognition approach in cognitive-IoT system," *Multimed Tools Appl*, vol. 80, no. 17, pp. 26273–26296, Jul. 2021, doi: 10.1007/s11042-021-10932-x.

[23] Z. Zhao and A. Kumar, "A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features," *Pattern Recognit*, vol. 93, pp. 546–557, 2019, doi: 10.1016/j.patcog.2019.04.010.

[24] R. W. Jalal and M. F. Ghanim, "Enhancement of Iris Recognition System using Deep learning," in *2022 IEEE Symposium on Industrial Electronics & Applications (ISIEA)*, IEEE, Jul. 2022, pp. 1–7. doi: 10.1109/ISIEA54517.2022.9873666.

ISSN 2636-9680
eISSN 2682-9266

OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
53 – 62

Zero-Day Attacks Detection in Smart Community through Interoperability and Explainable AI

Tawhidur Rahman[1], and Mohammad Sayduzzaman[2]
[1]BGD e-GOV CIRT
[2]National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka-1350
[1]pial@cirt.gov.bd, BGD e-GOV CIRT

ARTICLE INFO

Article History
Received 23 Jun 2024
Received in revised form 27 Jun 2024
Accepted 23 Jul 2024

Keywords:
Zero-day Attack, Intrusion Detection System, Artificial Intelligence, Internet of Everything, Explainable AI, Cybersecurity, Interoperability, Data Analysis.

ABSTRACT

Abstract—Systems, technologies, protocols, and infrastructures all face interoperability challenges. It is among the most crucial parameters to give real-world effectiveness. Organizations that achieve interoperability will be able to identify, prevent, and provide appropriate protection on an international scale, which can be relied upon. This paper aims to explain how future technologies such as 6G mobile communication, Internet of Everything (IoE), Artificial Intelligence (AI), and Smart Contract embedded WPA3 protocol-based WiFi-8 can work together to prevent known attack vectors and provide protection against zero-day attacks, thus offering intelligent solutions for smart cities. The phrase "zero-day" refers to an attack that occurs on the "day zero" of the vulnerability's disclosure to the public or vendor. Existing systems require an extra layer of security. In the security world, interoperability enables disparate security solutions and systems to collaborate seamlessly. AI improves cybersecurity by enabling improved capabilities for detecting, responding, and preventing zero-day attacks. When interoperability and Explainable Artificial Intelligence (XAI) are integrated into cybersecurity, they form a strong protection against zero-day assaults. Additionally, we evaluate a couple of parameters based on the accuracy and time required for efficiently analyzing attack patterns and anomalies.

I. INTRODUCTION

Attackers frequently use zero-day exploits to obtain unauthorized system access, steal sensitive information, disrupt services, or execute malicious code without being detected. As there is no prior information or defense against zero-day vulnerabilities, these attacks can be extremely harmful and difficult to remediate. Existing signature-based detection systems prove inefficient against zero-day attacks due to the Lack of Signatures, no prior knowledge, and, most importantly, poly-morphic characteristics of malware [1]. While some attackers employ methods like polymorphism, which alters virus properties over time, signature-based systems find it challenging to detect any anomalies or attacks. The anomaly-based detection system also failed to detect the newest attack as it lacks historical data as well as a sensitivity vs. false positive attitude. Attackers may employ sophisticated evasion techniques or mimic legitimate traffic to avoid triggering alerts and, most importantly, limited scope, which may not be adequately covered by the conventional detection system [2]. AI algorithms can effortlessly combine and analyze network logs, user activity analytics, endpoint security tools, and other data sources. This comprehensive approach improves threat detection accuracy. AI can swiftly assess data from interoperable systems and automate the reaction to zero-day assaults, minimizing the time window for an attacker to exploit the vulnerability. Interoperability enables companies and security systems to work together and share threat intelligence. In this research, we present an approach that combines interoperability with explainable artificial intelligence (XAI) to discover an optimal solution for detecting zero-day attacks [3].

ISSN 2636-9680
eISSN 2682-9266

Interoperability facilitates seamless communication between disparate systems. This is necessary to combine different technologies into a coherent network, including Wi-Fi 8, 6G, and the Internet of Everything IoE [4]. Fig. 1 explains the concept of interoperability in the context of technology, which refers to making sure that various platforms, networks, and devices can communicate with each other and function as a single unit, particularly in the areas of networking and cybersecurity. Systems can cooperate regardless of the underlying architecture when they are constructively interoperable [5]. Creating integrated networks—especially helpful for IoE ecosystems and multi-network environments—where different devices and technologies coexist and collaborate requires cross-platform interoperability. Through the facilitation of unified threat identification and response, interoperability can enhance security. Faster incident response and a wider understanding of security threats are made possible by this shared knowledge. Information sharing between systems makes it simpler to identify and address security risks, such as zero-day attacks. Interoperability guarantees that new technologies can be integrated into current systems with minimal effort [6].

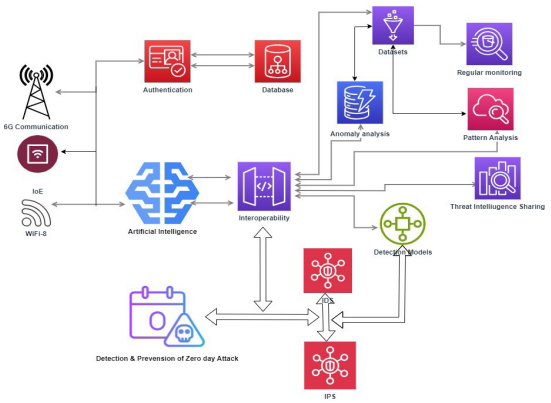

Fig. 1: Concept of Zero-day attack detection through interoperability, and AI

A cyberattack that leverages an undiscovered software vulnerability is known as a zero-day assault. Because the vulnerability is unknown to the software vendor or security community, no patch or remedy was available at the time of the attack. Fig. 2 describes the life cycle of a zero-day attack, highlighting its essential stages [7]:

- **Search and Discover**: A zero-day vulnerability is found by an individual or group, such as a researcher, hacker, or member of a security organization. The discovery could be made by code analysis, fuzzing, or exploiting other security issues

Fig. 2: Life Cycle of a Zero Day Attack

- **Development and Weaponizing**: Once the vulnerability has been identified, attackers create an exploit to take advantage of it. This entails writing code or developing a method for exploiting the vulnerability to infiltrate systems. In some circumstances, attackers may tailor the exploit to specific targets or conditions.
- **Deploy and Explore**: The exploit is converted into a format that can be utilized in a real-world attack. This could include generating malware, incorporating the exploit into existing malware, or launching a phishing effort to deliver the exploit to targets. Attackers frequently package their exploits to avoid detection by security software.
- **Impact and Disclosure**: Exploitation of the zero-day vulnerability can have serious implications. This could include data breaches, ransomware attacks, financial losses, espionage, and other harmful acts. The impact is often determined by the importance of the target, the sort of data or systems compromised, and the attacker's goals.
- **Response, Mitigation, and Learning**: The software provider provides a patch or upgrade to address the vulnerability. This approach can take some time, particularly if the vulnerability is complicated or impacts key systems. Security teams may undertake postmortem investigations to determine how the zero-day attack occurred, assess its tactics, and identify security process improvements to prevent such attacks in the future.

Though this is a well-renowned life cycle, an attacker might change or skip any steps mentioned here. An Intrusion Detection and Prevention System (IDPS) operates by keeping an eye on system activity or network traffic, analyzing collected data for threats using a variety of techniques, identifying potentially malicious traffic, notifying relevant personnel of identified threats, taking appropriate action

to stop intrusions once they are discovered, and producing reports for analysis and compliance. IDPS faces significant challenges in detecting zero-day attacks, as zero-day take advantage of undiscovered vulnerabilities, which prevents IDPS from having the required signatures or patches. Zero-day attacks do not have the known threat signatures that traditional signature-based IDPS rely on, making these systems unreliable against them. In our proposed methodology to overcome this issue, we introduced an intermediate layer between interoperability and the IDPS system that added an extra layer of defense through XAI to detect the zero-day attack. The main contribution of the paper is–

- To boost IDPS's overall performance, this work couples Artificial Intelligence with interoperability among sixth- generation (6G), WiFi-8, and IoE.
- The authors focus on Zero-Day attack pattern detection by combining Machine Learning with Explainable AI (XAI).
- In addition, they evaluate multiple models and consolidate the results for further investigation.

Organization: This paper is structured as follows: Discussions on the previous research and the concept of Interoperability among 6G, IoE & Wifi-8 in section II, Zero-day attack and its lifecycle to prevent the attack finally after weaponizing phase. Then, the proposed AI-based IDPS for zero-day attack detection, along with prevention and procedures, is presented in section III. The dataset description part is presented in section IV. Moreover, results and a related discussion are given in section V. Lastly, section VI contains the conclusion and some thoughts, limitations, and future scopes.

II. RELATED WORK

Intrusion Detection Systems have been essential in identifying any abnormal or suspicious activity that could compromise general security and pave the way for significant cyberattacks since the invention of Wi-Fi technology [8]. Many researchers employ various techniques to identify and stop zero-day attacks [9]. A few work with heuristic analysis, others with behavioral analysis, others with signature-based detection, others with threat intelligence, others with endpoint protection, others with advanced threat detection solutions, and others with cloud-based solutions [10].

Kumar et al. [11] study discussed parameters that are overlooked when identifying zero-day attacks. By omitting those requirements, several organizations claim they can manage complex cyberattacks but not in practical scenarios. By ignoring those requirements, we are merely avoiding the risk, and the attacker manages to complete his mission. Hindy et al. [12] use a deep learning-based methodology to identify zero-day attacks, with the primary risk being that the decision-making process frequently misses or fails to detect the true attack. Similarly, M. Macas et al. [13] focused on different deep learning technologies for detecting attacks in various perspectives.

Zhang et al. [14] showed how aggregated vulnerability- based assessment could detect zero-day attacks. Martins et al.
[15] worked on a host-based detection system. Another paper Salim et al. [16] implemented federated learning based detection system for healthcare. Zahoora et al. [17] mitigated XML injection based zero day attack via strategy-based detection system. On the other hand, Efe et al. [18] shows the comparison of host-based and network-based detection systems and what their limitations are. IDPS may be anomalous or signature-based as Nie et al. [19] focused on existing strategies and their loopholes. Recently, they began combining different technologies, such as SC and ML, to boost performance. We will describe the adoption process for AI and interoperability, followed by a review of previous work.

From the above discussion, we summarise that Numerous publications on Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) based on ML & AI were discovered throughout our investigation on this subject [20]. In certain articles, AI and ML are combined for IDS or IPS. However, there aren't many papers that show how interoper-ability among cutting-edge state-of-the-art technology with AI provides threat detection feeds for IDPS that prevent zero-day attacks [21]. That is the reason for our actions. For intrusion detection, we address XAI along with recent technologies.

ISSN 2636-9680
eISSN 2682-9266

III. PROPOSED METHODOLOGY FOR INTEROPERABILITY AND EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI)-BASED IDPS

In the constantly changing field of cyber security, one of the most dangerous risks that businesses and individuals encounter is the feared zero-day attack. The vendors are left with little time to create and implement a patch since these attacks make use of flaws in hardware, software, or firmware that they are unaware of. Hence, until a fix is released, hackers may take advantage of these vulnerabilities to obtain unauthorized access, interfere with business processes, or steal sensitive data. To overcome this issue, we developed an explainable artificial intelligence (XAI) based zero-day attack detection system given in Fig. 3. Most importantly, the proposed methodology is divided into three sections: the generic layer, the intermediate layer, and the final detection layer. In the generic layer, real-time thread intelligence of smart community systems (Wi-Fi8, IoE, 6G communication) is shared by interoperability to the intermediate layer. In the intermediate layer, we made use of machine learning techniques with XAI to create a robust zero-day attack detection system. The final layer analyzes the threat level and sends alerts to security teams through the IDPS system efficiently.

A. Generic Layer Discussion with Interoperability and Zero- Day Attacks

In case of cybersecurity, interoperability is the capacity of various hardware, software, and application platforms to efficiently exchange data, collaborate, and communicate with one another. It shares real-time threat intelligence, providing a more robust and timely response to emerging threats that can lead to faster identification of potential zero-day attacks. Interoperable security solutions allow for the correlation of events between various systems and network segments [22]. This connection can assist in identifying trends or abnormalities that might point to the existence of a zero-day attack that one system might not be able to detect. For example, if IoE detects suspicious activity that could be a zero-day attack, it can inform other systems like 6G communication and Wi-Fi8 to take preventative action without human intervention. Users are always creating data, a large amount of data is generated per day which is about 100 zettabytes [23] by Wi-fi8, IoE sensors, and 6G communication systems. To manage this large data most efficiently and securely in the generic layer, we used interoperability, which connects with the intermediate layer through real-time thread sharing.

B. Intermediate Layer Detection through ML and XAI Training Process

As previously described, zero-day attacks are mostly unpredictable by conventional ML and IDPS techniques, as their pattern is unrecognizable. To address this issue, in our proposed method, we applied explainable AI (XAI), which enables human users to transparently and easily comprehend the decisions and behaviors of AI systems with a high degree of learning performance (accuracy). From the generic layer, we will get the real-time sharing threat (data) and create a training database for generating shape value via XAI. In machine learning, SHAP (SHapley Additive exPlanations) values are a technique for analyzing any model's prediction.

In this paperwork, we apply XAI techniques on the dataset given in to generate two SHAP values, one for anomaly analysis and another for attack pattern analysis, which is the most significant feature for zero-day attack detection. In this dataset, there are nearly 45 attributes that are responsible for anomaly detection and attack pattern analysis. After applying XAI, we get 15 optimal attributes given in 4 and 5, indicating the contribution of each feature that is responsible for the attack and its pattern. In both figures, the Y-axis indicates the list of features that are highly responsible for the attack and its pattern detection, while the X-axis represents the severity index of the list of features. Both the SHAP values are generated based on the equation 1 given below [24] :

$$f(x) = \sum_{i=1}^{F} \phi_i + E_x[f(x)] \quad (1)$$

Where the model has p features, and ϕi is the SHAP value for feature i. According to this

equation, the average prediction and the total of all SHAP values equal the prediction for that particular occurrence.

Fig. 4 shows the SHAP values that are responsible for attack pattern detection, which is the main contribution of our work. As we know, zero-day cannot be identified because it has no known pattern. However, XAI can detect the features that are responsible for the attack pattern and detect newly encountered attack patterns very efficiently. On the other hand, Fig. 5 shows the SHAP values that are responsible for anomaly detection, which is also possible in conventional IDPS systems. However, after applying XAI the required computational time is decreased, on the contrary accuracy increased. This approach works as a two-layered detection system, the known attack patterns which already available are detected in this layer by the ML approach. As the zero-day is not possible to detect in this manner, it is passed to the final detection layer. As newly encountered zero-day attack patterns are identified via XAI in the intermediate layer and passed to the final detection layer, they can easily be identified via the IDPS technique.

The intermediate layer is the main contribution of this paperwork, which resolves the issues of the IDPS system in case of detection of a zero-day attack. As the pattern of zero- day is unknown, it cannot be resolved by a conventional IDPS system, that's why we introduced an intermediate layer where unknown zero-day attack patterns are detected in an efficient manner and passed to the IDPS to detect in the final layer detection system. Step by step, the working procedure for preventing zero-day attacks is mentioned as follows–

- Step 1 (Infrastructure Setup): Create a network structure that combines all 6G connections, IoE devices, and Wi-Fi 8 access points. Configure a multi-layered security system that includes firewalls, IDS/IPS, and endpoint protection.
- Step 2 (Data collection): Establish real-time thread sharing through interoperability for all communication channels on 6G, IoE, and Wi-Fi 8 networks.
- Step 3 (Analysis): Use XAI with ML technologies to analyze network traffic and detect anomalies in the intermediate layer. A Security Operations Center (SOC) or equivalent system should be used to monitor the network at all times [25]. All critical security-related incidents should be documented for further analysis and auditing.
- Step 4 (Detection and Alert): Monitor any unusual activities through IDPS techniques in the last layer then compare and check it with the treat intelligence stream. Provide security alerts using SOC if any anomaly occurs in the communication system.
- Step 5 (Recovery): Maintain regular backups of essential data and develop recovery plans. Conduct a thorough analysis to determine the underlying cause of a zero-

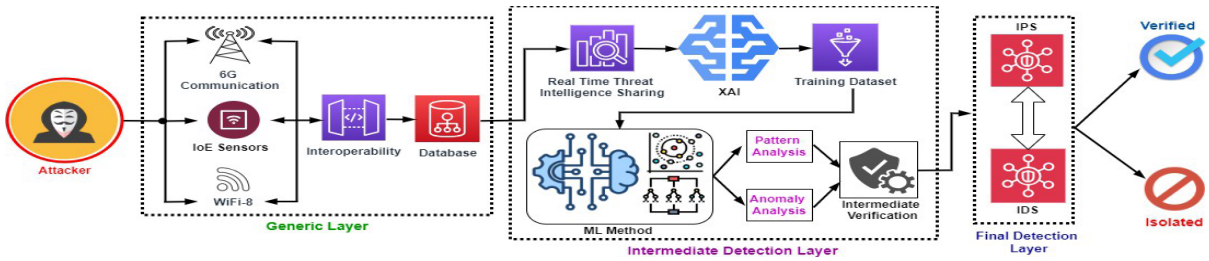

Fig. 3: Proposed Architecture for Interoperability and XAI-based IDPS

ISSN 2636-9680
eISSN 2682-9266

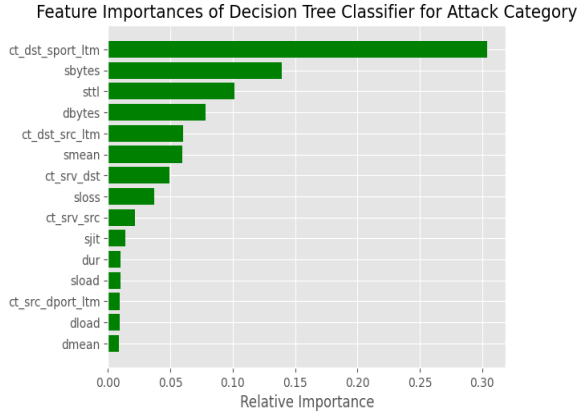

Fig. 4: SHAP values for Attack Pattern Analysis

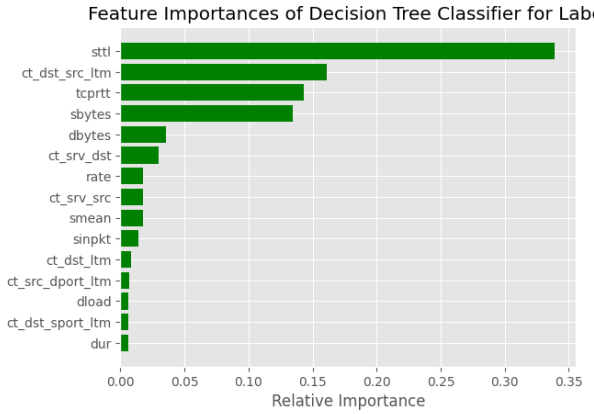

Fig. 5: SHAP values for Anomaly Analysis

day attack. Apply the appropriate updates and remedial measures to address vulnerabilities.

C. Final Layer Anomaly Detection with IDPS Technique

The types of attacks that are undetectable in the inter- mediate layer, like zero-day, will be detected in the final detection layer. As mentioned earlier, zero-day can not be detected by conventional IDPS systems, so we introduced an intermediate layer between interoperability and IDPS that will detect the newly encountered zero-day attack pattern using XAI techniques. This pattern will be passed to the IDPS system and it will block the user if there is any anomaly, otherwise pass the user normally. One of the most commonly used metrics is utilized in this work to assess the efficiency of intrusion detection models accuracy [26].

IV. DATASETS DESCRIPTION

This section focused on the proposed framework from a variety of perspectives and datasets. Initially, cupKDD99 was used to detect an intrusion. The effect of detection on performance is examined. The parameters with the best results are then picked for comparison with the centralized approach. The SHAP results are then used to explain and understand the outcomes of the proposed framework. The study concludes with a thorough discussion of the findings, providing insightful interpretations. NSL-KDD datasets are used to determine the categories of different types of attacks [27]. The NSL-KDD dataset is commonly utilized in intrusion detection and cybersecurity research. It is an improved version of the original KDD Cup 1999 dataset, which addresses some of its shortcomings. The KDD Cup 1999 dataset was built on a simulation of a military network and had various flaws, including excessive redundancy and poor representation of contemporary network traffic. The NSL-KDD dataset over-comes these shortcomings by presenting a more balanced and realistic depiction of network traffic. It is frequently used to assess intrusion detection systems (IDS) and machine learning models in the context of cybersecurity. Despite its improvements over the original KDD Cup 1999 dataset, NSL-KDD still contains certain flaws, such as redundant features and a lack of representation for some attacks.

UNSW-NB15 is used for network traffic feature extraction [24]. The UNSW-NB15 dataset is another extensively used dataset in network security and intrusion detection. It was developed by academics at the University of New South Wales (UNSW) in Australia and is specifically intended for evaluating network intrusion detection systems (NIDS). Another type of intrusion detection is host-based detection systems (HBDS). The dataset is based on network traffic recorded in a controlled setting, which may not accurately reflect the complexity and variety of real-world network traffic. As a result, models trained on this dataset may not perform well in real-world circumstances. Though it has some limitations, it is very helpful for security researchers. We use this dataset to check if our system is able to detect any unknown attacks. The result is

satisfactory as the system can successfully detect unknown attacks and prevent them by successfully isolating from the entire network through IDPS. The ToN-IoT dataset is a useful resource for evaluating the effectiveness of AI-enabled cybersecurity applications across IoT, network traffic, and operating systems [28]. The ToN-IoT dataset, like other intrusion detection datasets, may suffer from class imbalance, in which the number of cases reflecting typical traffic outnumbers those showing malicious or aberrant behavior. This mismatch can have an impact on the performance of machine learning models as well as how assessment results are interpreted [29].

V. RESULT ANALYSIS AND PERFORMANCE MEASUREMENT

In Table I, we compared our proposed work with some of the existing work considered during the background study. Moreover, for the experimental analysis in this work, the following parameters are used while measuring the performance and analyzing the results.

- Security Metrics: Security metrics include zero-day at- tack detection rate, false positive rate, incident response time, attack surface reduction, and anomaly detection accuracy. The accuracy is calculated by using Equation 2.'

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

- Efficiency Metrics: It focuses on resource consumption, network latency, algorithm processing time, and scalability.
- Effectiveness: It includes Threat prevention rate, attack vector identification, Incident resolution rate, and defensive capability.
- Continuous Improvement: We prioritize feedback loop efficacy, patch management efficiency, and security training impact for optimal performance.

A. ML Model and Accuracy of Attack Patterns Analysis

As we know zero-day attack is unrecognizable because it has no known pattern based on which we can perform a machine-learning approach. To overcome this issue we developed an XAI-based methodology, that can find out any unknown/newly generated pattern, which is not possible in any regular approach. Through the XAI to get the zero-day attack pattern we generate the SHAP value as given in Fig.4. The attributes/features that we get from the SHAP values are passed to several ML techniques which identify/detect the pattern that is newly encountered. In our dataset there are several attack categories, from there in the training phase we pass three attack categories called Normal, Dos, and Fuzzers. Among them Dos, and Fuzzers are anomalies, and Normal is not anomaly type at all. In the testing phase, we passed a new category of attack called Blackdoor which is detected by several ML techniques as shown in the Fig. 6. Among them, AdaBoostM1 shows the highest accuracy in the case of attack pattern detection as shown in Fig. 7.

B. Accuracy and Time of Anomaly Analysis

As discussed earlier, our proposed method can detect anomalies as a conventional IDPS system in the intermediate layer, yet in a more efficient manner with reduced computational time and improved accuracy. In the case of accuracy from Fig.8, we assert that without XAI, all of the ML models perform less accurately than with XAI, and similar cases also happen for the time factor. In the case of time, after applying XAI for some ML models like LogitBoost and DecisionTable,

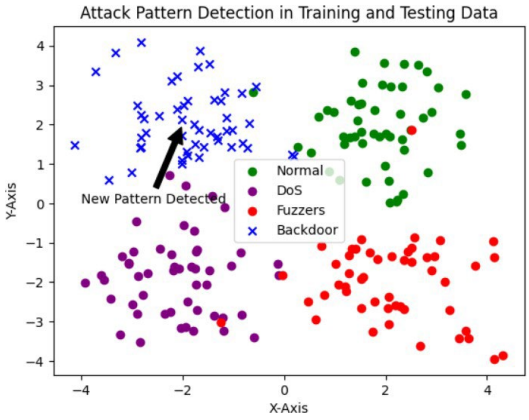

Fig. 6: Attack Pattern Detection

ISSN 2636-9680
eISSN 2682-9266

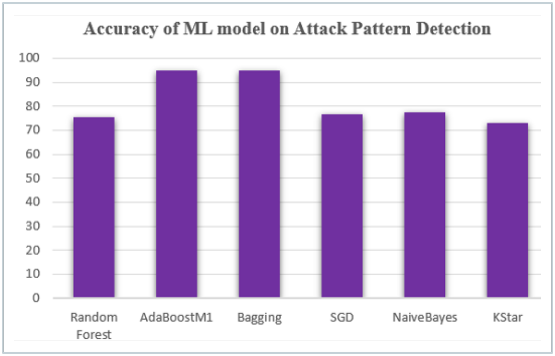

Fig. 7: Accuracy Matrics of ML Mode

time drastically fell, which indicates a significant reduction in computational time. Thus, we can say two objectives, attack pattern detection, and anomaly detection both are performed correctly in an efficient manner.

Fig. 8: Accuracy difference and Time efficiency

VI. CONCLUSION

Zero-day is the most vulnerable attack in the cyber security system. It can not be detected by a regular system, as its pattern is unknown and unrecognizable. To address this issue in the smart community in combination with interoperability, we introduce an intermediate layer that detects the unknown pattern of zero-day by XAI and supplies it to the IDPS system, which detects the anomaly. Furthermore, this intermediate layer works as double-layer anomaly detection, where regular attacks are detected in this layer in a more efficient way in the case of time and accuracy, and zero-day is detected in the final layer as XAI detects the pattern and passes it to the IDPS system. In the case of zero-day pattern detection, AdaBoostM1 performed the highest accuracy, whereas in anomaly detection, RandomSubspace triggered the highest accuracy for both with and without XAI. LogitBoost and DecisionTable take the lowest computational time after applying XAI in case of anomaly detection. The objectives that we mentioned before have been successfully completed using our proposed methodology. It can detect any kind of attack, including the most vulnerable zero-day. In the future, we will work on zero-day attack prevention with a larger dataset.

Sarhan et al. [30]	24,3064	MLP and RF	One Class	85.5%
Hindy et al. [12]	19,663	SVM and Autoencoders	One Class	92.96%
Kumar et al. [11]	53,234	Hitter and Graph Technique	Multi Class	88.98%
Koroniotis et al. [31]	18,563	Decision Tree	Binary	93.2%
Zahoora et al. [17]	16382	CSPE-R Ensemble	Binary	93%
Ashraf et al. [32]	18,563	FSVM	Multi Class	92%
Proposed Method	18,563	XAI and ML	Multi Class	94.89%

TABLE 1: Comparison of the proposed framework with the other state of art models

VII. REFERENCES

[1] A. Kumar and B. K. Chaurasia, "Detection of sars-cov-2 virus using lightweight convolutional neural networks," Wireless Personal Communications, vol. 135, no. 2, pp. 941–965, 2024.

[2] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artificial Intelligence Review*, vol. 56, no. 10, pp. 10 733–10 811, 2023.

[3] A. Rizzardi, S. Sicari, A. C. Porisini *et al.*, "Nero: Neural algorithmic reasoning for zero-day attack detection in the iot: A hybrid approach," *Computers & Security*, p. 103898, 2024.

[4] A. Rahman, T. Debnath, D. Kundu, M. S. I. Khan, A. A. Aishi, S. Sazzad, M. Sayduzzaman, and S. S. Band, "Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities," *AIMS Public Health*, vol. 11, no. 1, pp. 58–109, 2024.

[5] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari, and N. Kumar, "Impacts of blockchain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," *International Journal of Communication Systems*, p. e5429, 2023.

[6] F. Jinhong, "Cross-platform and multi-terminal collaborative software information security strategy," in *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. IEEE, 2024, pp. 781–787.

[7] K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, "Preventive determination and avoidance of ddos attack with sdn over the iot networks," in *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, 2021, pp. 1–6.

[8] R. Kishore and A. Chauhan, "Intrusion detection system a need," in *2020 IEEE International Conference for Innovation in Technology (INOCON)*, 2020, pp. 1–7.

[9] K.-A. Tait, J. S. Khan, F. Alqahtani, A. A. Shah, F. Ali Khan, M. U. Rehman, W. Boulila, and J. Ahmad, "Intrusion detection using machine learning techniques: An experimental comparison," in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, 2021, pp. 1–10.

[10] K. Saurabh, S. Sood, P. A. Kumar, U. Singh, R. Vyas, O. Vyas, and R. Khondoker, "Lbdmids: Lstm based deep learning model for intrusion detection systems for iot networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 753–759.

[11] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," Complex & Intelligent Systems, vol. 7, no. 5, pp. 2211–2234, 2021.

[12] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," Electronics, vol. 9, no. 10, p. 1684, 2020.

[13] M. Macas and C. Wu, "Review: Deep learning methods for cyber security and intrusion detection systems," in 2020 IEEE Latin-American Conference on Communications (LATINCOM), 2020, pp. 1–6.

[14] C. Zhang, Y. Chen, Y. Meng, F. Ruan, R. Chen, Y. Li, and Y. Yang, "A novel framework design of network intrusion detection based on machine learning techniques," Security and Communication Networks, vol. 2021, no. 1, p. 6610675, 2021.

[15] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes, and J. Gama, "Host-based ids: A review and open issues of an anomaly detection system in iot," Future Generation Computer Systems, vol. 133, pp. 95– 113, 2022.

[16] M. M. Salim, Y. Sangthong, X. Deng, and J. H. Park, "Articlesfederated learning-enabled zero-day ddos attack detection scheme in healthcare 4.0," vol. 14, 2024.

[17] U. Zahoora, A. Khan, M. Rajarajan, S. H. Khan, M. Asam, and T. Jamal, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive pareto ensemble classifier," Scientific Reports, vol. 12, no. 1, p. 15647, 2022.

[18] A. Efe and ˙I. N. Abacı, "Comparison of the host based intrusion detection systems and network based intrusion detection systems," pp. 23–32, 2022.

[19] J. Nie, P. Ma, B. Wang, and Y. Su, "A covert network attack detection method based on lstm," in 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), 2020, pp. 1690–1693.

[20] M. A. Talukder, K. F. Hasan, M. M. Islam, M. A. Uddin, A. Akhter, M. A. Yousuf, F. Alharbi, and M. A. Moni, "A dependable hybrid machine learning model for network intrusion detection," Journal of Information Security and Applications, vol. 72, p. 103405, 2023.

[21] C. Redino, D. Nandakumar, R. Schiller, K. Choi, A. Rahman, E. Bowen, A. Shaha, J. Nehila, and M. Weeks, "Zero day threat detection using graph and flow based security telemetry," in 2022 International Confer- ence on Computing, Communication, and Intelligent Systems (ICCCIS), 2022, pp. 655–662.

[22] A. Rahman, K. Hasan, D. Kundu, M. J. Islam, T. Debnath, S. S. Band, and N. Kumar, "On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," Future Generation Computer Systems, vol. 138, pp. 61–88, 2023.

[23] J. Edvardsson, "A survey on automatic test data generation," in Proceedings of the 2nd Conference on Computer Science and Engineering, 1999, pp. 21–28.

[24] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems:

ISSN 2636-9680
eISSN 2682-9266

Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set," Information Security Journal: A Global Perspective, vol. 25, no. 1-3, pp. 18–31, 2016.

[25] K. Demertzis, N. Tziritas, P. Kikiras, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: adaptive analytic lambda architecture for efficient defense against adversarial attacks," Big Data and Cognitive Computing, vol. 3, no. 1, p. 6, 2019.

[26] M. Soltani, B. Ousat, M. J. Siavoshani, and A. H. Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," Journal of Information Security and Applications, vol. 76, p. 103516, 2023.

[27] L. Dhanabal and S. Shantharajah, "A study on nsl-kdd dataset for intrusion detection system based on classification algorithms," International journal of advanced research in Computer and communication engineering, vol. 4, no. 6, pp. 446–452, 2015.

[28] N. Moustafa, "A new distributed architecture for evaluating ai-based security systems at the edge: Network ton iot datasets," Sustainable Cities and Society, vol. 72, p. 102994, 2021.

[29] A. Rahman, M. S. I. Khan, A. Montieri, M. J. Islam, M. R. Karim, M. Hasan, D. Kundu, M. K. Nasir, and A. Pescape`, "Blocksd-5gnet: Enhancing security of 5g network through blockchain-sdn with ml-based bandwidth prediction," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 4, p. e4965, 2024.

[30] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero- shot machine learning to zero-day attack detection," International Jour- nal of Information Security, vol. 22, no. 4, pp. 947–959, 2023.

[31] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for internet of things networks: A particle deep framework," Future Generation Computer Systems, vol. 110, pp. 91–106, 2020.

[32] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4507–4518, 2020.

OIC-CERT Permanent Secretariat:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

secretariat@oic-cert.org
www.oic-cert.org