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.

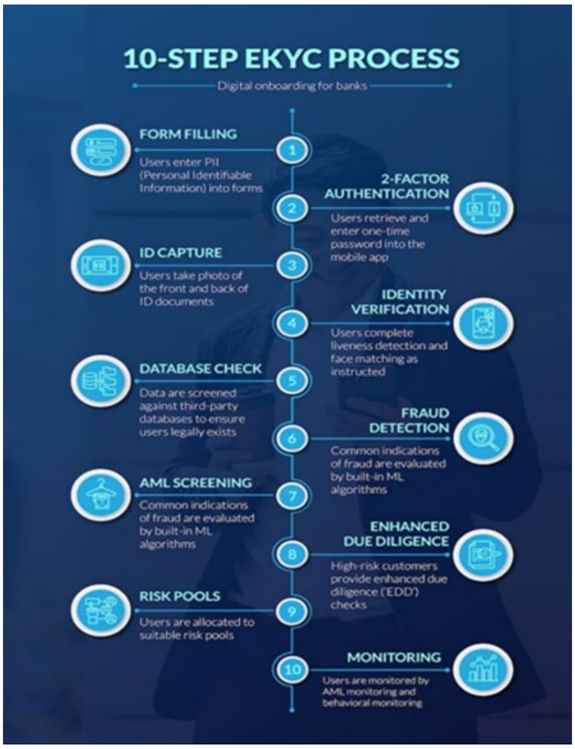
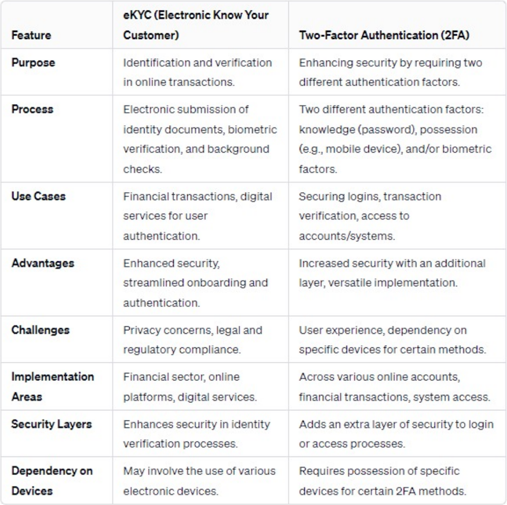

10-STEP EKYC PROCESS
Digital onboarding for banks
1
FORM FILLING
Users enter PII (Personal Identifiable Information) into forms
2
2-FACTOR AUTHENTICATION
Users retrieve and enter one-time password into the mobile app
3
ID CAPTURE
Users take photo of the front and back of ID documents
4
IDENTITY VERIFICATION
Users complete liveness detection and face matching as instructed
5
DATABASE CHECK
Data are screened against third-party databases to ensure users legally exists
6
FRAUD DETECTION
Common indications of fraud are evaluated by built-in ML algorithms
7
AML SCREENING
Common indications of fraud are evaluated by built-in ML algorithms
8
ENHANCED DUE DILIGENCE
High-risk customers provide enhanced due diligence ('EDD') checks
9
RISK POOLS
Users are allocated to suitable risk pools
10
MONITORING
Users are monitored by AML monitoring and behavioral monitoring

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 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

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).

[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.