JOURNAL OF DIGITAL SYSTEM DEVELOPMENT

https://e-journal.uum.edu.my/index.php/jdsd

How to cite this article:
Salmi Hassan & Adi Affandi Ahmad (2026). Verisigndoc: Digital Signature Verification System for Official Documents. *Journal of Digital System Development, 4* (1), 108-120. https://doi.org/10.32890/jdsd2026.4.1.8

VERISIGNDOC: DIGITAL SIGNATURE VERIFICATION SYSTEM FOR OFFICIAL DOCUMENTS

[1]Salmi Hassan & [2]Adi Affandi Ahmad

[1 & 2] School of Computing, Universiti Utara Malaysia, Malaysia

[1]Corresponding author: salmihassann@gmail.com

Received: 30/1/2026 Revised: 10/4/2026 Accepted: 10/4/2026 Published: 30/4/2026

ABSTRACT

The widespread adoption of digital documents in academic, governmental, and organisational environments has introduced significant challenges related to document authenticity, integrity, and trust. Conventional document approval processes often rely on manual signing or unsecured signature images, which are vulnerable to forgery, duplication, and unauthorised modification, underscoring the need for a secure, reliable digital document verification mechanism. This study presents VeriSignDoc, a web-based digital signature verification system designed to ensure the authenticity and integrity of official documents using cryptographic techniques based on Public Key Infrastructure (PKI). The system enables authorised users to digitally sign documents, while recipients can verify the validity of digital signatures through a verification interface without requiring prior registration. A usability evaluation and user acceptance testing were conducted with 30 participants from diverse academic backgrounds, who performed task-based activities, including document upload, digital signing, and document verification, followed by a structured Likert-scale questionnaire to assess usability, system functionality, and user interface quality. The findings indicate high levels of user satisfaction, ease of use, and functional reliability, with most participants agreeing that the system workflow was simple, verification results were clear and understandable, and the interface appeared professional and trustworthy. Overall, the results demonstrate that VeriSignDoc provides a practical, low-cost, and user-friendly solution for enhancing trust in digital document handling and verification processes.

Keywords: digital signature, document verification, PKI, system usability, web-based system.

INTRODUCTION

The increasing reliance on digital documents in academic, governmental, and organisational environments has transformed the way official information is created, shared, and approved. Official documents such as certificates, confirmation letters, vouchers, and institutional records are now commonly distributed in digital form to improve efficiency and accessibility (Shemshuchenko et al., 2019). However, this shift towards digital documentation has raised critical concerns about document authenticity, integrity, and trust, as digital files can be easily altered or duplicated without leaving visible evidence of modification.

In many organisations, document approval processes continue to rely on handwritten signatures or scanned signature images. While these methods are familiar and widely accepted, they are inherently insecure in digital environments, as signature images can be reused, manipulated, or impersonated for unauthorised purposes (Thangavel, 2023). Furthermore, the common practice of printing documents for manual signing, then scanning and reuploading them is time-consuming and inefficient, particularly in remote or time-sensitive workflows. This manual process also exposes documents to additional security risks during handling and transmission (Sulistiani et al., 2025).

Digital signatures have been recognised as a secure cryptographic mechanism for ensuring document authenticity and integrity in electronic communication. Unlike traditional signatures, digital signatures use cryptographic key pairs to bind a signer's identity to a document, ensuring that any post-signing modification can be detected (Tay & Goh, 2006). Public Key Infrastructure (PKI) further enhances this mechanism by providing a framework for secure key management, certificate issuance, and verification processes, thereby strengthening trust in digital transactions (Maddin & Anuar, 2022).

Several existing systems have successfully implemented PKI-based digital signature verification in real-world applications. For instance, Malaysia's e-Filing and MyTax systems employ digital certificates and PKI to ensure the confidentiality and integrity of tax-related documents (Lembaga Hasil Dalam Negeri Malaysia, 2022). Similarly, commercial platforms such as Adobe Acrobat Sign and DocuSign offer advanced digital signature solutions that comply with international standards. However, these systems are often restricted to specific domains, require paid digital certificates or subscription-based services, and may lack flexibility for broader use across different sectors (Adobe, n.d.; DocuSign, Inc., n.d.).

These limitations highlight the need for a secure, accessible, and cost-effective digital signature verification system that can be used beyond specialised or enterprise-level applications. In response to this need, this study proposes VeriSignDoc, a web-based digital signature verification system that enables users to securely and efficiently sign and verify official documents. VeriSignDoc utilises PKI and cryptographic hashing techniques to ensure that each digital signature is unique, verifiable, and resistant to forgery (Thangavel, 2023). The system supports authorised signers and unregistered verifiers, allowing document recipients to validate authenticity through a simple verification interface.

The objectives of this study are threefold: (1) to identify the requirements for a secure digital signature verification system, (2) to develop a functional prototype of the VeriSignDoc system, and (3) to evaluate the usability and ease of use of the system through user acceptance testing. By integrating strong security mechanisms with a user-centred design approach, this study aims to enhance trust in digital document management and contribute a practical solution for secure digital communication.

PREVIOUS WORK

The adoption of digital signature technologies has increased significantly in recent years due to the growing need for secure, efficient, and trustworthy digital document management. Digital signatures are widely used to ensure document authenticity, integrity, and non-repudiation in electronic transactions, particularly in sectors such as government, finance, and corporate administration (Tay & Goh, 2006). By utilising cryptographic algorithms and key pairs, digital signatures provide stronger security guarantees compared to traditional handwritten or scanned signatures, which are vulnerable to forgery and reuse (Thangavel, 2023).

Public Key Infrastructure (PKI) plays a crucial role in enabling secure digital signature implementation. PKI provides a framework for managing digital certificates, public and private keys, and certificate authorities (CAs), ensuring that digital signatures can be verified with confidence (Maddin & Anuar, 2022). In PKI-based systems, a signer uses a private key to generate a digital signature, while the recipient verifies the signature using the corresponding public key. Any modification to the signed document after the signing process invalidates the signature, thereby preserving document integrity (Tay & Goh, 2006).

One prominent example of a PKI-based digital signature system is Malaysia's e-Filing and MyTax platform operated by Lembaga Hasil Dalam Negeri Malaysia (LHDN). The MyTax system requires users to register and activate a valid digital certificate issued by trusted certificate authorities such as CTOS and DigiCert (Lembaga Hasil Dalam Negeri Malaysia, 2022). This approach ensures a high level of security and compliance with government regulations. However, the system is designed specifically for tax-related transactions and lacks flexibility for general document usage outside the government sector (LogMasuk.my, n.d.). Furthermore, a study by A. Rahman et al. (2018) reported that reliability did not significantly influence user satisfaction in the e-Filing system, suggesting that technical robustness alone may not be sufficient to ensure positive user perception without clear feedback and usability considerations.

Commercial digital signature solutions such as Adobe Acrobat Sign and DocuSign have also demonstrated the effectiveness of digital signature technologies in professional environments. Adobe Acrobat Sign supports certificate-based digital signatures using X.509 certificates and advanced standards such as PDF Advanced Electronic Signatures (PAdES), as well as secure hashing algorithms like SHA-256 (Adobe, n.d.). These features make Adobe Acrobat Sign widely accepted in legal and audit contexts. Nevertheless, the requirement for paid licenses and external digital certificates can be a barrier for small organisations and individual users seeking cost-effective solutions (Adobe, n.d.).

Similarly, DocuSign offers a comprehensive digital signature platform that supports multiple signature standards, including electronic signatures and qualified electronic signatures, and complies with international regulations such as eIDAS and ESIGN (DocuSign, Inc., n.d.). DocuSign is known for its user-friendly interface and strong system integration capabilities through application programming interfaces (APIs). Despite these advantages, the platform operates primarily as a subscription-based cloud service, with many advanced security features limited to enterprise-level plans, making it less accessible for users with limited budgets or offline requirements (DocuSign, Inc., n.d.).

While existing systems demonstrate the maturity and reliability of digital signature technologies, several limitations remain. Many solutions are either domain-specific, costly, or overly complex for general users. In addition, some systems prioritise security implementation while placing less emphasis on usability and user experience, which can affect user acceptance and adoption (A. Rahman et al., 2018). These gaps

highlight the need for a digital signature verification system that balances strong security mechanisms with simplicity, accessibility, and affordability.

In response to these limitations, the proposed VeriSignDoc system aims to provide a low-cost, web-based digital signature verification solution that leverages established cryptographic techniques such as PKI and secure hashing algorithms while maintaining a user-friendly interface. Unlike existing systems that require paid subscriptions or domain-specific integration, VeriSignDoc is designed to support a wide range of document types and use cases, including academic, organisational, and business documents. By focusing on both security and usability, VeriSignDoc seeks to extend the applicability of digital signature verification beyond specialised platforms and contribute to more trustworthy digital document management practices.

The increasing reliance on digital documents across academic, governmental, and organisational environments has amplified the importance of secure document handling and verification mechanisms. As official documents are frequently used as legal, academic, and administrative evidence, any compromise to their authenticity or integrity may lead to serious consequences, including misinformation, financial loss, and reputational damage (Shemshuchenko et al., 2019). Therefore, developing a secure digital signature verification system is critical to supporting trustworthy digital communication.

The VeriSignDoc system contributes significantly by providing a practical solution to the widespread problem of document forgery and signature impersonation in digital environments. By utilising Public Key Infrastructure (PKI) and cryptographic hashing algorithms, the system ensures that digitally signed documents can be verified accurately and that any unauthorised modification can be detected immediately (Tay & Goh, 2006; Thangavel, 2023). This capability addresses the limitations of conventional approval methods that rely on handwritten or scanned signatures, which are vulnerable to reuse and manipulation.

From an organisational perspective, VeriSignDoc offers a low-cost and accessible alternative to existing commercial digital signature solutions. Many established platforms require paid digital certificates, subscription-based services, or enterprise-level licensing, which may not be feasible for small organisations or individual users (Adobe, n.d.; DocuSign, Inc., n.d.). In contrast, VeriSignDoc is a web-based system that focuses on essential digital signature and verification capabilities without imposing high financial or technical barriers. This makes the system suitable for wider adoption across sectors such as education, small businesses, and public institutions.

In addition, the system supports both authorised signers and unregistered verifiers, enabling recipients to verify document authenticity without requiring system registration. This feature enhances usability and builds trust among recipients of documents, particularly those with limited technical knowledge of cryptographic systems. By simplifying the verification process while maintaining strong security mechanisms, VeriSignDoc bridges the gap between technical robustness and user accessibility (Maddin & Anuar, 2022).

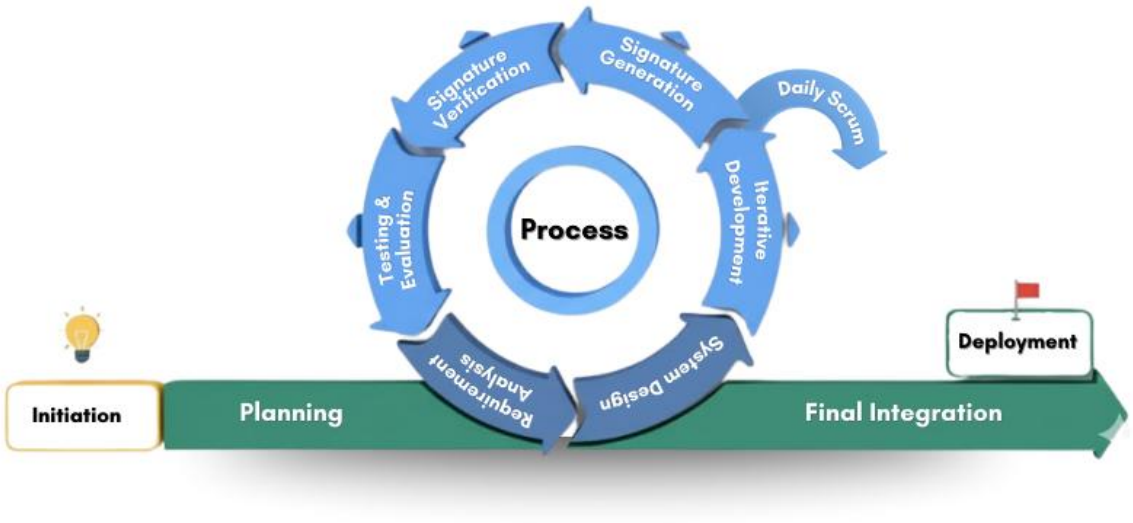
Overall, the significance of this project lies in its contribution to improving trust, efficiency, and security in digital document management. VeriSignDoc not only supports secure document approval and verification but also promotes awareness of digital signature technologies and best practices among users. The system aligns with ongoing digital transformation initiatives and provides a scalable foundation for future enhancements in secure digital communication.

METHODOLOGY

This study adopts the Agile Software Development Methodology to guide the design, development, and evaluation of the VeriSignDoc system. Agile methodology was selected for its flexibility, iterative development cycles, and emphasis on continuous feedback, which are well-suited to developing a secure web-based system within the scope and time constraints of a Final Year Project (Kukhnavets, n.d.). The methodology enables incremental development, early issue identification, and refinement of system features based on user and supervisor feedback. Figure 1 illustrates the iterative Agile-based development process adopted in this study, highlighting continuous planning, development, testing, and integration activities carried out across multiple development sprints.

Figure 1

An iterative Agile development process for VeriSignDoc using Scrum practices.



System Development Approach

The development of VeriSignDoc was carried out using an iterative sprint-based approach adapted from Scrum practices. The project was divided into multiple development sprints, each focusing on specific tasks such as requirement analysis, system design, module implementation, testing, and refinement. Initial sprints focused on understanding system requirements and designing the overall architecture, followed by the implementation of core functionalities, including digital signature generation, signature verification, and user interface development. Subsequent sprints focused on system integration, testing, and usability evaluation. This iterative approach allowed the system to evolve progressively while ensuring that functional and non-functional requirements were consistently addressed. Continuous testing and integration during each sprint helped improve system reliability and usability before proceeding to the next development phase.

Cryptographic Design and Security Mechanism

VeriSignDoc employs Public Key Infrastructure (PKI) as the foundation for its digital signature mechanism. PKI enables secure management of public and private keys, ensuring that digital signatures can be reliably generated and verified (Tay & Goh, 2006). In the signing process, a document is first processed using a secure hashing algorithm to generate a unique hash value. This hash value is then encrypted using the signer's private key to produce a digital signature. Any modification to the document after signing results in a different hash value, thereby invalidating the signature during verification.

The system utilises the SHA-256 cryptographic hash algorithm, which is widely recognised for its security and resistance to collision attacks (Thangavel, 2023). During verification, the system decrypts the digital signature using the signer's public key and compares the resulting hash with a newly generated hash of the received document. If both values match, the document is confirmed as authentic and unaltered. This mechanism ensures document integrity, authenticity, and non-repudiation.

System Architecture and Functional Scope

VeriSignDoc is implemented as a web-based application, allowing users to access the system through standard web browsers without additional software installation. The system supports two main user roles: signers, who are registered users authorised to digitally sign documents, and verifiers, who are recipients that can verify document authenticity without system registration. Each signed document includes a verification mechanism that enables recipients to check signature validity through the system interface.

The system's functional scope includes document upload, digital signature generation, digital signature verification, and the display of verification results. Non-functional requirements such as usability, accessibility, and security were also considered throughout the development process to ensure a positive user experience.

Usability Evaluation and User Acceptance Testing

To evaluate the effectiveness of the VeriSignDoc system, a usability evaluation and user acceptance testing (UAT) were conducted. A total of 30 participants were involved in the evaluation, consisting of undergraduate students from various academic backgrounds. Participants were selected to represent both users with prior experience in digital document handling and those without technical expertise, ensuring a balanced assessment of system usability.

Participants were required to perform predefined task-based scenarios, including uploading a document, digitally signing the document, and verifying the signed document. Upon completing the tasks, participants responded to a structured questionnaire administered using a Likert-scale format to assess system usability, functionality, and user interface quality. Open-ended questions were also included to gather qualitative feedback and suggestions for system improvement.

Data Collection and Analysis

The data collected from the usability evaluation were analysed using descriptive analysis techniques. Quantitative data from the Likert-scale questionnaire were summarised using percentages and frequency distributions to identify overall user perceptions and trends. Qualitative feedback from open-ended responses was reviewed to identify recurring themes related to usability, system clarity, and user

satisfaction. The results of this analysis provide insights into the system's performance, strengths, and areas for potential enhancement.

ANALYSIS AND RESULTS

This section presents the findings obtained from the usability evaluation and user acceptance testing conducted on the VeriSignDoc system. The analysis focuses on participant demographics, system usability, functionality performance, and user interface evaluation. Descriptive statistical methods were used to analyse quantitative data collected through Likert-scale questionnaires. At the same time, qualitative feedback from open-ended questions was reviewed to provide additional insights into user perceptions and system performance.

Participant Demographics

A total of 30 participants took part in the field testing of the VeriSignDoc system. The participants represented users with varying levels of experience handling digital documents, ranging from beginners to advanced users. This diversity ensured that the system was evaluated across different user experience levels, reflecting its suitability for general use.

In terms of gender distribution, the majority of participants were female (96.7%), while male participants accounted for 3.3% of the total respondents. The age group analysis showed that most participants were between 20 and 24 years old (76.7%), followed by those aged 30 years and older (20%), with a smaller proportion aged 25 to 29 years. Regarding educational background, most participants held a Bachelor's degree (86.7%), followed by Diploma holders (10%), with a small number holding a Master's degree. These results indicate that the evaluation primarily involved participants with tertiary-level education, which is appropriate for assessing a system designed for handling official digital documents.

Participants' academic backgrounds were diverse, with more than half of the respondents (53.3%) from Computer Science, followed by Information Technology (10%), and the remaining participants from non-IT disciplines. Additionally, participants reported varying levels of experience with digital documents: beginner (33.3%), intermediate (40%), and advanced (26.7%). Slightly more than half of the participants (53.3%) had prior experience using digital signature systems, while the remaining participants (46.7%) had no prior experience. This balanced distribution supports the validity of the usability evaluation, as both experienced and first-time users were included.

Table 1

Demographic profile of study participants (n = 30)

Variable	Category	Frequency (n)	Percentage (%)
Gender	Female	29	96.7
	Male	1	3.3
Age Group	20-24 years	23	76.7

	25-29 years	1	3.3
	≥ 30 years	6	20.0
Education Level	Diploma	3	10.0
	Bachelor's Degree	26	86.7
	Master's Degree	1	3.3
Field of Study	Computer Science	16	53.3
	Information Technology	3	10.0
	Non-IT	11	36.7
Experience with Digital Documents	Beginner	10	33.3
	Intermediate	12	40.0
	Advanced	8	26.7
Prior Experience with Digital Signatures	Yes	16	53.3
	No	14	46.7

Usability Evaluation Results

The usability evaluation results indicate a positive overall perception of the VeriSignDoc system. Most participants agreed that the system was easy to use and that they learned it quickly. Responses to the questionnaire showed that the system workflow was perceived as simple and easy to follow, allowing users to complete tasks without confusion or difficulty.

Participants also reported a high level of confidence when using the system independently, indicating that minimal guidance or technical assistance was required. Overall satisfaction levels were high, with most respondents selecting "Agree" or "Strongly Agree" when asked about their satisfaction with the VeriSignDoc system. These findings suggest that the system successfully meets usability expectations and provides an intuitive experience for users with varying levels of technical knowledge.

Table 2 summarises the usability evaluation results of the VeriSignDoc system. The majority of participants reported positive perceptions across all usability items, with more than 90% agreeing that the system was easy to use, easy to learn, and provided clear verification results.

Table 2

Summary of usability evaluation results (n = 30)

Usability Item	Agree (%)	Neutral (%)	Disagree (%)
The system is easy to use	93.3	6.7	0.0
The system is easy to learn	90.0	10.0	0.0
The workflow is clear and understandable	93.3	6.7	0.0
I can use the system without assistance	86.7	13.3	0.0
The verification results are clear and easy to interpret	93.3	6.7	0.0
Overall, I am satisfied with the system	90.0	10.0	0.0

System Functionality Performance

The evaluation of system functionality demonstrated that the core features of the VeriSignDoc system operated reliably during testing. Most participants agreed that the document upload function worked correctly and consistently. The digital signing process was reported to function smoothly, with users successfully applying digital signatures to documents without encountering critical errors.

In addition, participants perceived the document verification function to be accurate and effective. The system's verification results were considered clear and understandable, enabling users to determine whether a document was valid or invalid easily. The majority of participants also reported no critical system errors during testing, indicating the system's stability and reliability under normal usage conditions.

As shown in Table 3, the core functionalities of the VeriSignDoc system performed reliably during evaluation, with all participants completing document upload and digital signature verification tasks.

Table 3

System functionality performance evaluation (n = 30)

System Function	Successful (%)	Neutral (%)	Unsuccessful (%)
Document upload	100.0	0.0	0.0
Digital signature generation	96.7	3.3	0.0
Digital signature verification	100.0	0.0	0.0
Display of verification results	96.7	3.3	0.0
Overall system stability	93.3	6.7	0.0

User Interface Evaluation

The user interface (UI) evaluation results further support the positive reception of the VeriSignDoc system. Participants agreed that the system interface was visually clear, well-organised, and easy to navigate. The text, buttons, and labels were reported to be readable and understandable, contributing to efficient task completion.

Most respondents also perceived the system design as professional and trustworthy, which is particularly important for applications involving official documents and security-related processes. Furthermore, participants indicated they did not feel confused while navigating the system, suggesting that the overall layout and navigation structure effectively support user interaction and task flow.

Qualitative Feedback and User Suggestions

Qualitative feedback from open-ended questionnaire responses revealed that participants appreciated the system's simplicity, the clarity of verification results, and the convenience of completing digital signature tasks online. Common themes identified included ease of use, a straightforward workflow, and the system's trustworthiness.

Participants also provided constructive suggestions for improvement, such as adding clearer user guidance for first-time users, enhancing on-screen instructions, and refining certain interface elements. While several participants indicated that no improvements were necessary, these suggestions highlight potential areas for future enhancements and refinements to the VeriSignDoc system.

DISCUSSION

The findings from the usability evaluation and user acceptance testing demonstrate that the VeriSignDoc system successfully achieves its intended objectives of providing a secure, usable, and reliable digital signature verification platform. Overall, participants reported positive experiences when interacting with the system, indicating that the combination of strong cryptographic mechanisms and a user-centred interface design contributed to effective system adoption.

The high level of usability observed in the evaluation aligns with prior studies emphasising the importance of simplicity and clarity in security-related systems. Previous research has shown that users are more likely to trust and adopt digital security solutions when system workflows are intuitive and do not require extensive technical knowledge (Rahman et al., 2018). In the case of VeriSignDoc, participants were able to complete core tasks such as document upload, digital signing, and verification without assistance, suggesting that the system successfully bridges the gap between technical security implementation and practical usability.

From a functionality perspective, the reliable performance of digital signing and verification processes confirms the effectiveness of the PKI-based design adopted in this study. The use of cryptographic hashing and public–private key mechanisms ensured that document integrity and authenticity could be verified accurately, consistent with established digital signature principles described by Tay and Goh (2006). The clarity of verification results further enhanced user confidence, as participants could easily interpret whether a document was valid or invalid. This finding supports the argument that effective feedback mechanisms are essential for fostering trust in digital verification systems (Maddin & Anuar, 2022).

The positive user interface evaluation highlights the role of visual clarity and professional design in security systems handling official documents. Participants perceived the system as trustworthy, which is a critical factor for applications involving legal, academic, or administrative records. This observation is consistent with earlier findings that users' perceptions of professionalism and transparency significantly influence the acceptance of digital services, particularly in government and institutional contexts (Shemshuchenko et al., 2019).

Despite the generally positive outcomes, the qualitative feedback also revealed areas for potential improvement. Suggestions such as enhanced user guidance and clearer on-screen instructions indicate that first-time users may benefit from additional support when interacting with digital signature technologies. These findings are consistent with the literature, which suggests that even user-friendly security systems require adequate guidance to accommodate users with limited prior exposure to cryptographic concepts (Thangavel, 2023). Addressing these aspects in future system iterations could further improve usability and broaden system adoption.

Overall, the discussion of results suggests that VeriSignDoc effectively balances security, usability, and accessibility. By providing a low-cost, web-based solution that leverages established cryptographic standards while remaining easy to use, the system addresses key limitations identified in existing digital signature platforms. The findings reinforce the importance of integrating user experience considerations into secure system design and highlight VeriSignDoc's potential as a practical solution for enhancing trust in digital document management.

CONCLUSION

This study presented VeriSignDoc, a web-based digital signature verification system designed to enhance the authenticity, integrity, and trustworthiness of official digital documents. The system was developed in response to the growing challenges associated with document forgery, signature impersonation, and inefficient manual approval processes in digital environments. By integrating Public Key Infrastructure (PKI) and secure cryptographic hashing techniques, VeriSignDoc provides a reliable mechanism for digitally signing and verifying documents in a secure and user-friendly manner (Tay & Goh, 2006; Thangavel, 2023).

The findings from the usability evaluation and user acceptance testing indicate that VeriSignDoc successfully meets its design objectives. Results show high levels of user satisfaction, ease of use, and functional reliability across core system features, including document upload, digital signing, and signature verification. Participants were able to interact with the system confidently without requiring technical assistance, demonstrating that the system effectively balances strong security mechanisms with accessibility for non-technical users. These outcomes support previous studies highlighting the importance of usability and clear system feedback in promoting trust and adoption of digital security solutions (Rahman et al., 2018; Maddin & Anuar, 2022).

In addition, the positive perception of the system's interface and professional design reinforces the role of user experience in applications involving official and security-sensitive documents. By offering a low-cost, web-based alternative to existing commercial digital signature platforms, VeriSignDoc addresses key limitations in affordability and accessibility identified in prior systems, such as government-specific and

subscription-based solutions (Adobe, n.d.; DocuSign, Inc., n.d.). This makes the system suitable for broader adoption across academic institutions, small organisations, and general users.

Despite these contributions, this study is subject to certain limitations. The evaluation focused primarily on usability and user acceptance, while advanced security performance testing and large-scale deployment scenarios were beyond the scope of the current project. Future work may involve expanding system functionality, enhancing user guidance features, and conducting comprehensive security and performance evaluations. Overall, this study demonstrates that VeriSignDoc is a practical and effective solution for secure digital document verification and contributes to ongoing efforts to strengthen trust in digital document management practices.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Maddin, A. M., & Anuar, H. S. (2022). E-filing system effectiveness: Malaysia perspective. *Global Scientific Journal, 10*(1), 1131–1134. https://www.globalscientificjournal.com

Rahman, M. K. B. A., Othman, A. K., & Amrin, N. (2018). The effects of e-service quality on users' satisfaction: A case of e-Filing at LHDN. *International Journal of Engineering & Technology, 7*(3.15), 1–3. https://doi.org/10.1007/978-981-10-6053-3_9

Shemshuchenko, Y., Parkhomenko, N., Tarakhonych, T., Podorozhna, T., & Husariev, S. (2019). Official document as a legal act: Essential aspects. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 443–451.

Sulistiani, I., Al-Amin, & Nastiar, M. F. (2025). Professional communication in the digital age: Benefits and challenges of using instant messaging applications in the workplace. *International Journal of Society Reviews (INJOSER), 3*(2), 346–352. https://www.researchgate.net/publication/388790815

Thangavel, V. (2023). Use of digital signature verification system (DSVS) in various industries: Security to protect against counterfeiting. *Managerial and Decision Economics*. https://www.researchgate.net/publication/371083633

Adobe. (n.d.). *Certificate-based signatures*. Adobe Help Centre. https://helpx.adobe.com/acrobat/using/certificate-based-signatures.html

Adobe. (n.d.). *Digital IDs*. Adobe Help Centre. https://helpx.adobe.com/acrobat/using/digital-ids.html

DocuSign, I. (n.d.). *Implementing electronic signatures and digital signatures with DocuSign*. https://www.docusign.com/how-it-works/legality/global

DocuSign, I. (n.d.). *eSignature plans and pricing*. https://ecom.docusign.com/en-GB/plans-and-pricing/esignature

Kukhnavets, P. (n.d.). *Sprints in Scrum*. Hygger. https://hygger.io/guides/agile/scrum/sprints-in-scrum/

Lembaga Hasil Dalam Negeri Malaysia. (2022, October 30). *Panduan pengguna MyTax 2.0*. https://mytax.hasil.gov.my/

LogMasuk.my. (n.d.). *Cara mohon sijil digital LHDN untuk e-Filing, MyTax dan e-PCB*. https://logmasuk.my/sijil-digital-lhdn/

Tay, E. S., & Goh, C. Y. (2006). Legal issues and technical aspects of the digital signature mechanism in Malaysia. In *Proceedings of the International Conference on E-Commerce (ICoEC, 2006)* (pp. 82–88).