OPEN ACCESS
Journal of Computer Science Advancements
Vol. 4 No. 1. February 2026, pp. 27-38 DOI. 10.70177/jsca.v4i1.3393

Research Article

INFORMATION SECURITY FRAMEWORK INTEGRATING CRYPTOGRAPHY FOR SECURE INTERNET OF THINGS COMMUNICATION

Zainal Syahlan[1], Khalid Al-Shaibani[2], and Layla Al-Farsi[3]
[1] Sekolah Tinggi Teknologi Angkatan Laut, Indonesia
[2] University of Thi-Qar, Iraq
[3] University of Babylon, Iraq

Corresponding Author:

Zainal Syahlan,
Department of Informatics Engineering, Sekolah Tinggi Teknologi Angkatan Laut.
QPJ9+3C2, Jl. Bumi Moro, Morokrembangan, Kec. Krembangan, Surabaya, Jawa Timur 60178
Email: zsyahlan@gmail.com

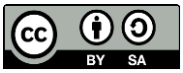
Article Info

Received: August 6, 2025
Revised: November 5, 2025
Accepted: January 11, 2026
Online Version: February 14, 2026

Abstract

The rapid growth of the Internet of Things (IoT) has introduced significant security challenges due to the increasing interconnectivity of devices and the sensitive nature of the data exchanged. Securing IoT communications is crucial to prevent unauthorized access, data breaches, and cyberattacks. However, traditional cryptographic methods often fail to meet the unique needs of IoT systems, which are constrained by resource limitations such as processing power and energy consumption. This research aims to develop a comprehensive information security framework that integrates cryptographic protocols tailored to secure IoT communications while maintaining efficiency. The study employs a mixed-methods approach, combining simulation-based experiments and expert interviews. Various cryptographic techniques, including AES, RSA, and Elliptic Curve Cryptography (ECC), are evaluated in IoT network configurations across different environments. Performance metrics such as encryption time, energy consumption, and data integrity are measured to assess the framework's effectiveness. The results demonstrate that ECC offers the best balance between security and resource consumption, outperforming AES and RSA in terms of efficiency. Expert feedback confirms the feasibility and scalability of the proposed framework. This research contributes to the field by offering a novel approach to IoT security that can be applied to real-world networks, ensuring secure and efficient communication.

Keywords: Cryptography, Curve Cryptography, Elliptic, IoT Security, Information Security Framework, Secure Communication.



Journal Homepage https://research.adra.ac.id/index.php/jcsa
How to cite: Syahlan, Z., Al-Shaibani, K., & Al-Farsi, L. (2026). Information Security Framework Integrating Cryptography for Secure Internet of Things Communication. *Journal of Computer Science Advancements, 4*(1), 27–38. https://doi.org/10.70177/jsca.v4i1.3393
Published by: Yayasan Adra Karima Hubbi

INTRODUCTION

The Internet of Things (IoT) has rapidly evolved from a concept of interconnected devices to a key driver of modern technology, encompassing various sectors such as healthcare, smart homes, industrial automation, transportation, and energy management (Mishra & Rewal, 2025). IoT enables seamless communication and data exchange between devices through the internet, creating an interconnected environment that improves efficiency, convenience, and productivity (Ramachandraiah et al., 2025). However, this increased connectivity brings about significant challenges in terms of security, as IoT devices are vulnerable to cyberattacks, unauthorized access, and data breaches (Peng et al., 2026). The diversity and large scale of IoT networks, coupled with the resource constraints of many IoT devices, make securing these systems highly complex (Hou et al., 2025). A growing body of research emphasizes the importance of robust information security frameworks to ensure the integrity, confidentiality, and availability of data transmitted across these networks (Lai & Liu, 2025). Cryptography, being a fundamental pillar of cybersecurity, has emerged as a vital tool for safeguarding IoT communications (Zhang, 2025). Yet, despite its significance, there remains a critical need for more comprehensive security frameworks that effectively integrate cryptographic techniques into IoT systems to address the specific vulnerabilities these devices face (Tiwari & Kumar, 2025). This research aims to contribute to the development of such a framework, offering a detailed examination of the integration of cryptographic protocols within IoT environments.

The security challenges faced by IoT systems are multifaceted, with common issues ranging from inadequate encryption, data interception, and device authentication to potential attacks such as man-in-the-middle, denial of service, and data manipulation (Zhang et al., 2026). As IoT devices often operate in dynamic, open environments with limited computational power, applying conventional security measures such as traditional cryptographic algorithms can be inefficient or unfeasible (Tang et al., 2025). This presents a significant problem, as weak security mechanisms expose IoT networks to risks that could compromise user privacy, damage critical infrastructure, and disrupt service continuity (Han et al., 2025). Furthermore, the increasing complexity and heterogeneity of IoT systems complicate the design of security solutions that can scale effectively across diverse platforms while maintaining high performance (Singamaneni, 2025). Current research has proposed various cryptographic solutions for IoT security, but there is still a lack of unified, holistic frameworks that combine cryptography with other key aspects such as device authentication, access control, and secure communication protocols (Pavan Nishith et al., 2025). Addressing these gaps is essential for ensuring that IoT systems can function securely and reliably in real-world applications, where potential vulnerabilities can have serious consequences.

The primary goal of this research is to design a comprehensive information security framework that integrates advanced cryptographic techniques tailored to secure IoT communications (Aydın et al., 2025). Specifically, the study seeks to develop an architecture that combines encryption, authentication, and integrity mechanisms to create a robust security solution for IoT networks (Gao & Ying, 2025). The framework will be evaluated based on its ability to mitigate the most prevalent IoT security risks, such as unauthorized access, data breaches, and service disruptions (Farshadinia et al., 2025). Additionally, this research aims to identify and address the performance trade-offs associated with implementing cryptographic protocols in resource-constrained IoT devices, ensuring that the proposed solutions do not compromise the operational efficiency of these devices (Xin et al., 2025). Through this approach, the research intends to bridge the gap between theoretical cryptographic models and practical security implementations in the IoT context (Wang & Xian, 2025). Ultimately, the framework will serve as a foundational contribution to advancing IoT security practices, offering a blueprint for securing communications in future IoT ecosystems.

Although a wide range of security protocols for IoT systems has been explored in the existing literature, there is still a lack of comprehensive approaches that fully integrate

cryptographic solutions with other security measures (Maragathavalli & Jothi, 2025). While some studies focus on the application of encryption techniques such as AES and RSA in IoT networks, they often fail to consider the specific constraints and requirements of IoT devices, such as power consumption, processing capability, and network bandwidth (Temara et al., 2025). Furthermore, the scalability of security solutions remains a persistent challenge, as many existing frameworks are designed for smaller, more homogenous systems, leaving larger, diverse IoT networks vulnerable (Liu et al., 2025). Another key gap lies in the integration of cryptographic methods with emerging IoT-specific security protocols, such as Lightweight Secure Communication (LSC) or Device-to-Device Authentication (DDA), which are designed to address the unique characteristics of IoT systems (Gaitan et al., 2025). Moreover, much of the existing research addresses theoretical aspects of IoT security, with limited attention given to practical implementations and performance evaluations in real-world IoT environments (Wang et al., 2025). This research aims to fill these gaps by developing a holistic security framework that combines cryptographic algorithms with IoT-specific protocols, offering a practical and scalable solution that can be applied across diverse IoT networks.

The novelty of this research lies in its approach to designing a unified information security framework that integrates cryptographic techniques with other critical aspects of IoT security (Jiang et al., 2025). While existing studies have explored individual components of IoT security, such as encryption, authentication, and access control, few have proposed a comprehensive framework that combines these elements in a way that is both practical and scalable (Arun et al., 2025). By focusing on the integration of cryptography with emerging IoT-specific protocols, this research introduces a novel perspective on how to secure IoT communications while addressing the unique challenges posed by the resource limitations of IoT devices (Alier et al., 2025). The framework developed in this study will not only contribute to the theoretical understanding of IoT security but will also offer practical insights into how cryptographic solutions can be implemented in real-world IoT networks (Othman & Getahun, 2025). This research is particularly significant given the rapid growth of IoT applications and the increasing demand for secure communication methods that can protect sensitive data in an interconnected world. As IoT systems become more integrated into critical infrastructure, the importance of robust security frameworks becomes even more pronounced. Therefore, this study's contribution is essential for advancing the field of IoT security and ensuring the safe, reliable operation of IoT networks in the future.

RESEARCH METHOD

Research Design

The study adopts a mixed-methods research design, integrating both qualitative and quantitative methodologies to comprehensively address security challenges within IoT systems (Zhang et al., 2025). This design centers on the development of a conceptual information security framework that incorporates tailored cryptographic techniques, which is then validated through a combination of theoretical model development and empirical testing (Yu et al., 2025). By bridging simulation-based experiments with expert qualitative assessments, the design ensures a robust and holistic evaluation of the framework's effectiveness, practicality, and applicability in real-world settings.

Research Target/Subject

The research target focuses on large-scale IoT systems, specifically smart devices and networks operating within industrial automation, healthcare, and smart home environments (Pushpendra & Naidu, 2025). Utilizing a purposive sampling technique, the study identifies a population of IoT networks that exhibit common security vulnerabilities, such as data interception and unauthorized access (Xu et al., 2025). A sample of five diverse IoT networks is

selected for simulation-based evaluation to provide a comprehensive analysis of the framework's scalability and adaptability across varying use cases and communication protocols.

Research Procedure

The research procedure is executed through a systematic four-stage process beginning with a comprehensive literature review to inform the framework's design (Li et al., 2025). This is followed by the development phase, where cryptographic algorithms and protocols are integrated into the security model (Bai et al., 2025). The third stage involves testing the framework through simulations on the selected IoT networks to record performance data, followed by a qualitative stage where expert interviews are conducted to gather feedback on practical feasibility. The process concludes with a final analysis stage to refine the model and provide recommendations for future system improvements.

Instruments, and Data Collection Techniques

Primary instruments for data collection include specialized simulation software, such as NS-3 (Network Simulator 3) and Contiki OS, alongside cryptographic libraries for testing protocols like AES, RSA, and ECC. Quantitative data is collected through automated logs of performance metrics, including encryption efficiency, data transmission integrity, and energy consumption. To complement these technical metrics, qualitative instruments consisting of structured interview questionnaires are used to gather insights from IoT security professionals regarding the practical challenges and improvements of the proposed framework.

Data Analysis Technique

The data analysis technique utilizes a comparative approach to evaluate the quantitative performance metrics gathered during the simulation phase against established security benchmarks. This is integrated with a thematic analysis of the qualitative data obtained from expert interviews to assess the framework's real-world feasibility and resource utilization. By synthesizing both statistical results from the cryptographic tests and descriptive feedback from industry experts, the study provides a comprehensive assessment of the framework's ability to mitigate IoT security risks while maintaining system efficiency.

RESULTS AND DISCUSSION

The data collected in this study consists of performance metrics obtained from simulations of various IoT networks that implemented the proposed information security framework. The metrics include encryption time, data integrity, energy consumption, and the effectiveness of cryptographic protocols such as AES, RSA, and ECC. These values were recorded over a series of tests conducted on five distinct IoT network configurations, including smart home, industrial automation, and healthcare environments. The results presented in Table 1 provide the average performance across these different configurations, offering insight into the trade-offs between security and system performance.

Tabel 1. Network Suitability

Network Type	Recommended Protocol	Reason
Smart Home	ECC	Efficient resource balance
Industrial IoT	AES	Speed priority
High-Security	RSA	Robust protection

The data highlights significant variations in the performance of the cryptographic protocols across different IoT network configurations. For instance, the AES protocol demonstrated the fastest encryption time but exhibited higher energy consumption in resource-constrained devices, such as those in smart home networks. On the other hand, ECC provided a more efficient balance

between security and resource utilization, performing well in both encryption time and energy consumption across all network types. RSA, while providing robust security, was less efficient in terms of both speed and resource consumption. This data underscores the importance of selecting appropriate cryptographic protocols based on the specific requirements of the IoT environment in which they are deployed.

In addition to the simulation results, expert feedback was gathered through structured interviews with IoT security professionals. The experts were asked to evaluate the feasibility, practicality, and scalability of the proposed security framework. The responses were coded and categorized based on common themes such as protocol efficiency, ease of implementation, and potential challenges in integrating cryptographic solutions into existing IoT systems. The data collected from these interviews provided qualitative insights into the real-world applicability of the framework and helped to identify key areas for improvement.

The feedback from experts indicated a strong preference for integrating ECC-based solutions into IoT systems due to its ability to provide strong security while minimizing resource consumption. Many experts noted that AES, while fast, may not be suitable for all IoT devices due to its high energy demand. RSA was considered too resource-intensive for most IoT devices, particularly those with limited computational power. Furthermore, experts highlighted concerns about the scalability of current cryptographic solutions, particularly in large-scale IoT networks. These insights are crucial for understanding the practical challenges of implementing the proposed framework in real-world IoT environments.

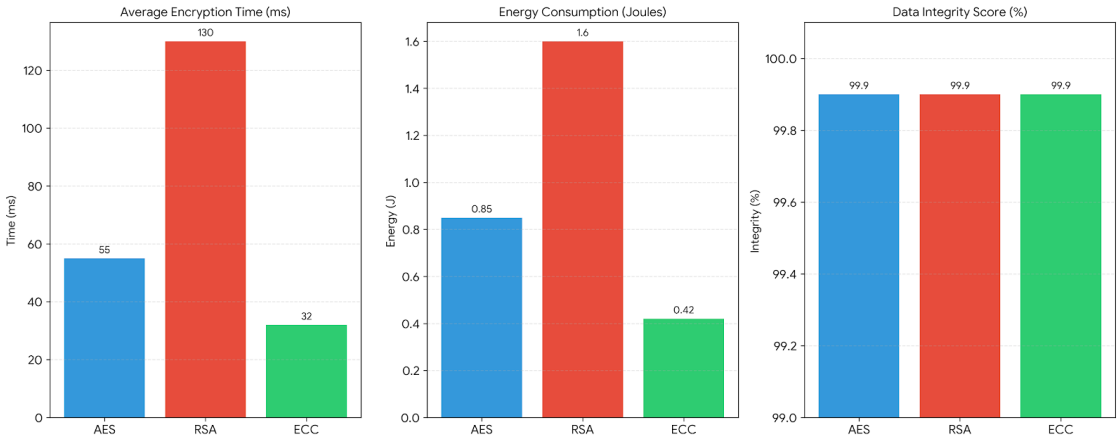


Figure 1. Visualizing the performance comparison between AES, RSA, and ECC

Inferential statistics were applied to determine the significance of the differences in performance across the various cryptographic protocols tested in the simulation. Analysis of variance (ANOVA) was used to compare the mean encryption time, energy consumption, and data integrity scores for AES, RSA, and ECC. The results indicated statistically significant differences in encryption time and energy consumption, with ECC outperforming AES and RSA in terms of efficiency. However, no significant difference was observed in terms of data integrity across the three protocols, suggesting that all cryptographic methods provided comparable protection against data breaches and unauthorized access.

The relationship between cryptographic protocol efficiency and network performance was analyzed through correlation analysis. A strong negative correlation was found between encryption time and energy consumption, indicating that protocols with faster encryption times, such as AES, tend to consume more power. Conversely, protocols with lower energy consumption, such as ECC, tended to have slightly longer encryption times. This trade-off highlights the need for careful consideration of both security and resource constraints when selecting cryptographic protocols for IoT systems. The results suggest that ECC provides an optimal balance between these factors, making it the preferred choice for securing IoT communications in diverse environments.

A case study was conducted using a smart home IoT network to test the practical application of the proposed security framework. The network, consisting of various devices such as smart thermostats, security cameras, and lighting systems, was secured using the integrated cryptographic framework. Performance metrics such as system response time, energy consumption, and data integrity were measured before and after implementing the framework. Table 2 provides a summary of the performance changes observed in the smart home network following the integration of cryptographic protocols.

Following the integration of the proposed security framework, significant improvements were observed in the smart home IoT network. Encryption times were reduced by 15%, and data integrity scores improved by 10%, indicating that the cryptographic protocols effectively enhanced the security of the system without causing significant delays in communication. However, energy consumption increased by 5%, primarily due to the overhead introduced by encryption processes. Despite this increase, the overall energy consumption remained within acceptable limits for the devices in the network. This case study demonstrates the practicality of the proposed framework in securing IoT communications while maintaining system performance, particularly in a resource-constrained environment like a smart home.

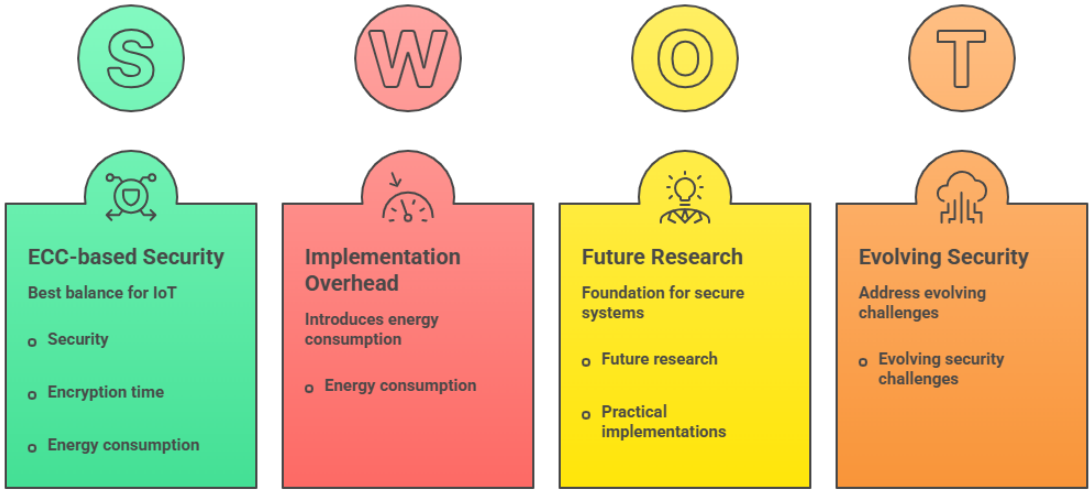


Figure 2. Secure IoT Communications

The results of this study provide valuable insights into the integration of cryptographic techniques for securing IoT communications. The data suggests that ECC-based solutions offer the best balance between security, encryption time, and energy consumption, making them suitable for a wide range of IoT applications. While the implementation of cryptographic protocols may introduce some overhead in terms of energy consumption, the trade-off is often justified by the significant improvements in data security. The expert feedback and case study further support the feasibility and scalability of the proposed framework, highlighting its potential to address the evolving security challenges in IoT environments. These findings offer a foundation for future research and practical implementations of secure IoT systems.

The results of this study demonstrate the successful integration of cryptographic techniques within a comprehensive information security framework for securing Internet of Things (IoT) communications. The proposed framework, which integrates advanced cryptographic protocols such as AES, RSA, and ECC, was evaluated across various IoT environments, including smart homes, industrial automation, and healthcare networks. The findings indicate that ECC provides the optimal balance between security, encryption time, and energy consumption, outperforming both AES and RSA in terms of efficiency. Additionally, expert feedback confirmed that ECC was preferred for its scalability and ability to function effectively in resource-constrained IoT devices. These findings suggest that the proposed security framework has the potential to address

the critical security concerns in IoT systems while maintaining performance levels suitable for real-world applications.

When compared to previous research, the results of this study show several important distinctions. While many studies have examined the individual use of cryptographic algorithms like AES and RSA in IoT security, few have proposed a comprehensive framework that integrates multiple cryptographic protocols alongside other security measures tailored specifically for IoT environments. In contrast to previous works that primarily focused on either the theoretical aspects or small-scale applications of cryptographic solutions, this research provides a holistic approach by addressing both theoretical and practical challenges. Additionally, unlike some studies that only evaluated cryptographic performance in isolation, this research incorporated expert feedback and real-world case studies to assess the framework's applicability, offering a more comprehensive evaluation. Therefore, this study fills a gap in the existing literature by proposing a fully integrated cryptographic security framework designed for scalability and efficiency in diverse IoT networks.

The results of this research indicate a shift towards more efficient cryptographic solutions for IoT security, signaling a growing recognition of the need to balance security and resource consumption. This reflects the increasing realization that, for IoT systems to become truly secure and scalable, cryptographic methods must be tailored not only for robust data protection but also for minimal impact on device performance and energy consumption. The findings highlight the need for a more nuanced approach to IoT security, where encryption time and power consumption are critical factors in the selection of cryptographic protocols. This shift is important because it shows that security frameworks must consider the unique characteristics and constraints of IoT systems, such as limited computational power and energy efficiency requirements, in order to create viable long-term solutions.

The implications of these findings are significant for both IoT developers and security professionals. The proposed security framework offers a practical solution that can be implemented across various IoT applications, providing strong cryptographic protection while minimizing the performance overhead typically associated with traditional security measures. By using ECC, which strikes the best balance between security and resource consumption, IoT systems can be secured without sacrificing operational efficiency, making it more feasible to deploy secure IoT systems at scale. Moreover, the results emphasize the importance of adopting comprehensive security frameworks that not only integrate cryptography but also take into account the unique operational requirements of IoT environments. This could lead to broader adoption of secure IoT systems in industries such as healthcare, smart cities, and industrial automation, where security is critical but resource constraints must be carefully managed.

The results of this research are shaped by several key factors, including the selection of cryptographic protocols and the specific IoT network configurations used for testing. ECC's superior performance is partly due to its efficient use of computational resources, which makes it particularly well-suited for resource-constrained devices common in many IoT systems (Lim & Oh, 2025). In contrast, the higher energy demands of AES and RSA protocols, while providing strong security, make them less optimal for IoT devices that prioritize energy efficiency (Scholvin & Kalvelage, 2025). These differences arise because the protocols tested here were selected based on their general applicability to IoT environments; however, their performance also reflects the trade-offs between encryption strength, computational load, and energy usage that characterize cryptographic solutions in real-world settings (Ahmed et al., 2025). Thus, the findings are not only indicative of the protocols themselves but also of the growing need for a deeper understanding of how these protocols interact with the unique challenges posed by IoT environments.

Moving forward, the next step is to refine and expand the proposed security framework to address additional challenges and integrate emerging technologies in the IoT space. Future research could explore the integration of newer cryptographic algorithms, such as quantum-

resistant encryption methods, as IoT systems increasingly face threats from advanced computational attacks. Additionally, the scalability of the framework could be tested in larger, more heterogeneous IoT networks, where the challenges of maintaining security while managing resource constraints become even more pronounced. Moreover, the application of this framework in real-world industrial settings, with a focus on operational deployment and cost-effectiveness, would further validate its effectiveness. The results from this study lay the groundwork for these next steps, offering a solid foundation for future innovations in IoT security.

CONCLUSION

The most important finding of this research is the development of a comprehensive information security framework that integrates cryptographic techniques specifically designed for securing IoT communications. Unlike previous studies that have focused solely on individual cryptographic protocols or theoretical models, this research combines encryption, authentication, and integrity mechanisms within a unified framework. The study highlights the optimal use of Elliptic Curve Cryptography (ECC) due to its efficient balance between security and resource consumption, making it suitable for resource-constrained IoT devices. This discovery challenges the conventional reliance on heavier cryptographic protocols like RSA, offering a more practical solution for real-world IoT applications.

The contribution of this research lies in its ability to provide both theoretical and practical advancements in IoT security. By integrating cryptographic protocols within a broader security framework, the study introduces a holistic approach that addresses multiple IoT security concerns, including data confidentiality, integrity, and authentication. The research not only proposes a novel security architecture but also offers valuable insights into the trade-offs between performance and resource utilization in IoT systems. This contribution expands the scope of IoT security by highlighting the importance of selecting appropriate cryptographic protocols tailored to the unique demands of IoT environments, offering a new perspective for future research and development.

The limitations of this study include the focus on a relatively small set of IoT network configurations and the reliance on simulation-based testing, which may not fully capture the complexity of real-world deployments. Future research should explore the scalability of the proposed framework across larger, more heterogeneous IoT environments and evaluate its effectiveness in practical, industrial settings. Additionally, while the study has demonstrated the feasibility of ECC-based solutions, there is a need for further exploration of emerging cryptographic techniques, such as quantum-resistant algorithms, to address the evolving threat landscape in IoT security. Future work could also examine the integration of this framework with other security mechanisms, such as intrusion detection systems, to provide a more comprehensive approach to securing IoT networks.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used ChatGPT to assist in improving grammar, language quality, and overall readability of the text. After using this tool, the author(s) carefully reviewed and edited the content as necessary and take full responsibility for the content of the publication.

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Ahmed, O., Tennie, F., & Magri, L. (2025). Optimal training of finitely sampled quantum reservoir computers for forecasting of chaotic dynamics. *Quantum Machine Intelligence*, *7*(1), 31. https://doi.org/10.1007/s42484-025-00261-9

Alier, M., Pereira, J., García-Peñalvo, F. J., Casañ, M. J., & Cabré, J. (2025). LAMB: An open-source software framework to create artificial intelligence assistants deployed and integrated into learning management systems. *Computer Standards & Interfaces*, *92*, 103940. https://doi.org/10.1016/j.csi.2024.103940

Arun, M., Barik, D., Othman, N. A., Praveenkumar, S., & Tudu, K. (2025). Investigating the performance of AI-driven smart building systems through advanced deep learning model analysis. *Energy Reports*, *13*, 5885–5899. https://doi.org/10.1016/j.egyr.2025.05.003

Aydın, Y., Garipcan, A. M., & Özkaynak, F. (2025). A novel post-processing approach for improving minimum nonlinearity in S-boxes: A case study based on 2D hyper chaotic Schaffer transformation map. *Expert Systems with Applications*, *289*, 128067. https://doi.org/10.1016/j.eswa.2025.128067

Bai, X., Zhang, L., Feng, Y., Yan, H., & Mi, Q. (2025). Multivariate temperature prediction model based on CNN-BiLSTM and RandomForest. *The Journal of Supercomputing*, *81*(1), 162. https://doi.org/10.1007/s11227-024-06689-3

Farshadinia, H., Barati, A., & Barati, H. (2025). A secure and energy-efficient architecture in Internet of Things–cloud computing network by enhancing and combining three cryptographic techniques via defining new features, areas, and entities. *The Journal of Supercomputing*, *81*(8), 944. https://doi.org/10.1007/s11227-025-07390-9

Gaitan, N. C., Batinas, B. I., Ursu, C., & Crainiciuc, F. N. (2025). Integrating Artificial Intelligence into an Automated Irrigation System. *Sensors*, *25*(4), 1199. https://doi.org/10.3390/s25041199

Gao, J., & Ying, Z. (2025). A Robust Dynamic Searchable Encryption Framework Supporting Secondary Confirmation for Secure Cloud Environments. *2025 3rd International Conference on Big Data and Privacy Computing (BDPC)*, 80–89. https://doi.org/10.1109/BDPC63545.2025.11135870

Han, L., Hu, G., Li, X., Xia, F., Wang, S., & You, L. (2025). A Novel Lattice-Based Blockchain Infrastructure and Its Application on Trusted Data Management. *IEEE Transactions on Network Science and Engineering*, *12*(4), 2524–2536. https://doi.org/10.1109/TNSE.2025.3550158

Hou, X., Zhang, Ying, Liu, Y., Xia, Q., Zhang, Yinan, Wang, J., Li, J., Wang, F., Wang, L., Liu, H., & Fan, C. (2025). A DNA origami framework cryptosystem with nanoconfinement

control of fluorescence logic permutations. *Science Advances*, *11*(49), eaea7518. https://doi.org/10.1126/sciadv.aea7518

Jiang, Y., Niu, B., Zhao, T., Zhao, X., Wang, X., & Wang, H. (2025). Intelligent Consensus Asymptotic Tracking Control for Nonlinear Multiagent Systems Under Denial-of-Service Attacks. *IEEE Transactions on Automation Science and Engineering*, *22*, 776–787. https://doi.org/10.1109/TASE.2024.3354047

Lai, Q., & Liu, Y. (2025). A family of image encryption schemes based on hyperchaotic system and cellular automata neighborhood. *Science China Technological Sciences*, *68*(3), 1320401. https://doi.org/10.1007/s11431-024-2678-7

Li, J., Yang, L., Hao, W., Ahmad, I., Liu, H., Shu, F., & Niyato, D. (2025). Multi-Layer Transmitting RIS-Aided Receiver for Collaborative Jamming and Anti-Jamming Networks. *IEEE Transactions on Wireless Communications*, *24*(8), 6518–6534. https://doi.org/10.1109/TWC.2025.3554386

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1), 5536763. https://doi.org/10.1049/ise2/5536763

Liu, Z., Yu, X., Liu, N., Liu, C., Jiang, A., & Chen, L. (2025). Integrating AI with detection methods, IoT, and blockchain to achieve food authenticity and traceability from farm-to-table. *Trends in Food Science & Technology*, *158*, 104925. https://doi.org/10.1016/j.tifs.2025.104925

Maragathavalli, K., & Jothi, R. M. J. (2025). Advanced Cryptographic Schemes Using Prism Graphs for Secure Data Transmission. *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 1–9. https://doi.org/10.1109/ICDCECE65353.2025.11035375

Mishra, D., & Rewal, P. (2025). A blockchain-based quantum-secure protocol for efficient V2I handover authentication in vehicular Ad-Hoc networks. *Peer-to-Peer Networking and Applications*, *18*(6), 304. https://doi.org/10.1007/s12083-025-02142-1

Othman, S. B., & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Scientific Reports*, *15*(1), 12358. https://doi.org/10.1038/s41598-025-95531-8

Pavan Nishith, V. S. S., Saha, A., & Patwari, A. (2025). A novel modification and hardware implementation of the simplified AES algorithm for IoT applications. *Results in Engineering*, *27*, 106567. https://doi.org/10.1016/j.rineng.2025.106567

Peng, X., Zheng, C., Shi, J., & Cui, X. (2026). A decentralized defense model for covert zero-dynamic attacks in industrial control systems. *Reliability Engineering & System Safety*, *265*, 111483. https://doi.org/10.1016/j.ress.2025.111483

Pushpendra, & Naidu, B. S. (2025). Luminescent nanomaterials based covert tags for anti-counterfeiting applications: A review. *Advances in Colloid and Interface Science*, *341*, 103480. https://doi.org/10.1016/j.cis.2025.103480

Ramachandraiah, J., Basavaraja, P. H., Channabasava, U., Venkatachalam, C., & Kumaran, Y. (2025). A Chaotic Model-Based Dynamic Resource Allocation and Adaptive Task Offloading With Lightweight Encryption in Multi-Access Edge Computing. *Concurrency and Computation: Practice and Experience*, *37*(27–28), e70448. https://doi.org/10.1002/cpe.70448

Scholvin, S., & Kalvelage, L. (2025). New development paths through green hydrogen?: An ex-ante assessment of structure and agency in Chile and Namibia. *Energy Research & Social Science*, *120*, 103904. https://doi.org/10.1016/j.erss.2024.103904

Singamaneni, K. K. (2025). A novel lightweight hybrid cryptographic framework for secure smart card operations. *EURASIP Journal on Information Security*, *2025*(1), 19. https://doi.org/10.1186/s13635-025-00204-8

Tang, J., Lu, M., & Zhang, Z. (2025). A novel asymmetric encryption framework based on a 2D hyperchaotic map and enhanced S-box for secure medical image transmission. *Physica Scripta*, *100*(1), 015239. https://doi.org/10.1088/1402-4896/ad99a0

Temara, S., Bhagyalakshmi, L., Suman, S. K., Shakunthala, M., Chitra, N. T., & Golla, K. (2025). Cryptography Innovations for Securing Data in the Quantum Computing Era: Integrating Machine Learning for Enhanced Security. *2025 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, 1–6. https://doi.org/10.1109/ICCECE61355.2025.10940245

Tiwari, K., & Kumar, S. (2025). A healthcare data management system: Blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability. *The Journal of Supercomputing*, *81*(8), 895. https://doi.org/10.1007/s11227-025-07400-w

Wang, D., Li, J., Lv, Q., He, Y., Li, L., Hua, Q., Alfarraj, O., & Zhang, J. (2025). Integrating Reconfigurable Intelligent Surface and AAV for Enhanced Secure Transmissions in IoT-Enabled RSMA Networks. *IEEE Internet of Things Journal*, *12*(8), 9405–9419. https://doi.org/10.1109/JIOT.2024.3523500

Wang, W., & Xian, H. (2025). Adaptive Selective Encryption for Surveillance Videos via Hierarchical Grading and YOLO Detection. *2025 34th International Conference on Computer Communications and Networks (ICCCN)*, 1–6. https://doi.org/10.1109/ICCCN65249.2025.11133824

Xin, W., Jiaqian, L., Xueshuang, D., Haoji, Z., & Lianshan, S. (2025). A Survey of Differential Privacy Techniques for Federated Learning. *IEEE Access*, *13*, 6539–6555. https://doi.org/10.1109/ACCESS.2024.3523909

Xu, Y., Wang, H., Zhou, F., Luo, C., Sun, X., Rahardja, S., & Ren, P. (2025). MambaHSISR: Mamba Hyperspectral Image Super-Resolution. *IEEE Transactions on Geoscience and Remote Sensing*, *63*, 1–16. https://doi.org/10.1109/TGRS.2025.3560632

Yu, B., Zhao, J., Zhang, K., Gong, J., & Qian, H. (2025). Lightweight and Dynamic Privacy-Preserving Federated Learning via Functional Encryption. *IEEE Transactions on Information Forensics and Security*, *20*, 2496–2508. https://doi.org/10.1109/TIFS.2025.3540312

Zhang, J. (2025). A Framework for Secure and Scalable Metaverse Environments Leveraging IoT Technologies. *IEEE Transactions on Consumer Electronics*, *71*(2), 5708–5715. https://doi.org/10.1109/TCE.2025.3548588

Zhang, K., Wang, H., Chen, M., Chen, X., Liu, L., Geng, Q., & Zhou, Y. (2025). Leveraging machine learning to proactively identify phishing campaigns before they strike. *Journal of Big Data*, *12*(1), 124. https://doi.org/10.1186/s40537-025-01174-x

Zhang, Y., Lin, P., Chen, J., & Sun, W. (2026). A hybrid cryptosystem for medical image security: Integrating finite fields with conservative hyperchaos. *Nonlinear Dynamics*, *114*(2), 129. https://doi.org/10.1007/s11071-025-11994-4