International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
Impact Factor (RJIF): 5.64
Journal's Website
IJCCN 2026; 7(1): 77-84
Received: 02-10-2025
Accepted: 05-11-2025

R Nandakumar
Associate Professor, PG Department of Computer Science, RV Government Arts College, Chengalpattu, Tamil Nadu, India

E Venkatesan
Guest Lecturer, PG Department of Computer Science, RV Government Arts College, Chengalpattu, Tamil Nadu, India

AN Swamynathan
Associate Professor, PG Department of Computer Science, RV Government Arts College, Chengalpattu, Tamil Nadu, India

Dr. V Thangavel
Dr. V Thangavel
Head-LIRC, St. Francis Institute of Management and Research, Mumbai, Maharashtra, India

Corresponding Author:
Dr. V Thangavel
Head-LIRC, St. Francis Institute of Management and Research, Mumbai, Maharashtra, India

A hybrid cryptographic approach for protecting wireless networks against passive and active attacks

R Nandakumar, E Venkatesan, AN Swamynathan And V Thangavel

DOI: https://doi.org/10.33545/27075923.2026.v7.i1b.127

Abstract
Wireless networks have become an essential part of modern communication systems, but their open transmission medium makes them highly vulnerable to security threats such as unauthorised access, passive eavesdropping, brute-force attacks, and man-in-the-middle attacks. Ensuring secure wireless communication is therefore a critical challenge. This study presents a cryptography-based safeguarding framework designed to protect wireless networks from both active and passive attacks. The proposed approach integrates strong encryption, secure key management, and authentication mechanisms to prevent unauthorised users from entering the network and accessing sensitive data. Several cryptographic algorithms, including AES, RSA, ECC, and SHA-based hashing techniques, are analysed to evaluate their effectiveness in wireless security environments. Among these, the Advanced Encryption Standard (AES) combined with Elliptic Curve Cryptography (ECC) for key exchange is identified as the most suitable solution due to its high security strength, low computational overhead, and resistance to brute-force and passive attacks. AES ensures data confidentiality, while ECC provides secure authentication and key distribution with minimal power consumption, making it ideal for wireless and resource-constrained devices. The proposed cryptographic safeguarding model significantly enhances network confidentiality, integrity, and access control, ensuring that only authorised users can participate in wireless communication. This approach offers a robust and efficient solution for securing wireless networks against evolving cyber threats.

Keywords: Wireless Network Security, Cryptography, AES, ECC, Passive Attack, Brute-Force Attack, Unauthorized Access

1. Introduction
Wireless networking has become a fundamental component of modern communication infrastructure, enabling seamless connectivity across personal, commercial, industrial, and governmental domains. Technologies such as Wi-Fi, mobile networks, wireless sensor networks, and Internet of Things (IoT) systems have transformed the way information is accessed, shared, and processed. The rapid expansion of wireless communication has brought significant advantages, including mobility, scalability, and cost efficiency. However, the same characteristics that make wireless networks flexible and convenient also expose them to a wide range of security vulnerabilities. Unlike wired networks, wireless communication relies on open transmission media, making it inherently susceptible to unauthorized access and malicious attacks.

As wireless signals propagate through free space, they can be intercepted by unintended recipients without physical access to the network infrastructure. This exposure significantly increases the risk of security breaches, particularly when sensitive or confidential data is transmitted. Unauthorized users can exploit weak security mechanisms to gain access to network resources, disrupt communication, or steal private information. Consequently, safeguarding wireless networks has become a critical research area, especially as cyber threats continue to evolve in complexity and scale.

One of the most prominent challenges in wireless network security is protecting data from passive and active attacks. Passive attacks involve silent interception of transmitted data, such as eavesdropping and traffic analysis, where attackers attempt to extract information without altering network operations. These attacks are difficult to detect because they do not interfere directly with data transmission. In contrast, active attacks include brute-force attacks, replay attacks, spoofing, denial-of-service attacks, and man-in-the-middle attacks, where adversaries actively manipulate or disrupt network communication. Both categories pose serious threats to the confidentiality, integrity, and availability of wireless networks.

Unauthorised access remains a major concern in wireless environments. Weak authentication mechanisms, poor key management, and outdated encryption protocols often allow attackers to penetrate wireless networks and impersonate legitimate users. Once access is obtained, attackers can monitor communication, inject malicious packets, or launch further attacks on connected devices. This problem is particularly severe in public wireless networks, enterprise environments, and IoT systems, where large numbers of devices communicate continuously with minimal human intervention. Therefore, robust security mechanisms are essential to ensure that only authorised users can participate in wireless communication.

Cryptography plays a vital role in addressing these security challenges. It provides mathematical techniques for securing data through encryption, authentication, and integrity verification. By converting plain data into unreadable ciphertext, cryptographic algorithms protect information from unauthorised disclosure even if the communication channel is compromised. Modern wireless security protocols rely heavily on cryptographic techniques to establish secure communication channels, manage encryption keys, and verify user identities. Without cryptography, ensuring privacy and trust in wireless communication would be nearly impossible.

Symmetric and asymmetric cryptographic algorithms form the foundation of wireless network security. Symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), use a single secret key for both encryption and decryption. These algorithms are known for their efficiency and high performance, making them suitable for real-time wireless communication. However, secure key distribution remains a challenge in symmetric systems, especially in large or dynamic networks. If the secret key is compromised, the entire communication becomes vulnerable to brute-force attacks and data leakage.

Asymmetric cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), address key distribution challenges by using separate public and private keys. These algorithms enable secure key exchange and authentication, ensuring that encryption keys are shared only between legitimate users. Among asymmetric methods, ECC has gained significant attention due to its strong security with smaller key sizes, which reduces computational overhead and power consumption. This property makes ECC particularly suitable for wireless networks, mobile devices, and IoT applications where resources are limited.

Hashing algorithms and message authentication techniques further enhance wireless network security by ensuring data integrity and authentication. Secure hash algorithms generate fixed-length hash values that detect any modification in transmitted data. When combined with encryption and digital signatures, hashing mechanisms help prevent replay attacks and unauthorised data alteration. These cryptographic tools collectively strengthen the overall security architecture of wireless networks.

Despite the availability of various cryptographic algorithms, selecting the most suitable approach for safeguarding wireless networks remains a complex task. Factors such as computational efficiency, energy consumption, resistance to brute-force attacks, and scalability must be carefully considered. Wireless devices often operate under constrained environments with limited processing power and battery life, which restricts the use of heavy cryptographic operations. Therefore, an optimal security solution must balance strong protection with minimal resource utilisation.

Recent research has shown that hybrid cryptographic frameworks offer an effective solution to wireless network security challenges. By combining symmetric encryption for data confidentiality with asymmetric cryptography for secure key exchange and authentication, hybrid models provide enhanced protection against both passive and active attacks. In such frameworks, AES is commonly used for encrypting data packets, while ECC is employed for secure key generation and distribution. This combination significantly reduces the risk of brute-force attacks and unauthorised access while maintaining high communication efficiency.

The increasing prevalence of cyberattacks targeting wireless networks highlights the need for continuous improvement in security mechanisms. Attackers are constantly developing new techniques to bypass traditional defences, exploit protocol weaknesses, and compromise encryption keys. As a result, outdated security protocols are no longer sufficient to protect modern wireless communication systems. Advanced cryptographic solutions must be adopted to ensure long-term network security and user trust.

This research focuses on safeguarding wireless networks using cryptographic algorithms to prevent unauthorized entry, passive eavesdropping, brute-force attacks, and other security threats. The study emphasises the evaluation of widely used cryptographic techniques and identifies the most suitable algorithms for wireless environments. By analyzing security strength, computational efficiency, and resistance to attacks, the research proposes a robust cryptographic framework that enhances confidentiality, integrity, and authentication in wireless communication. In summary, securing wireless networks is a critical requirement in today's interconnected world. Cryptography provides the essential tools needed to protect wireless communication from unauthorised users and malicious attacks. By adopting efficient and secure cryptographic algorithms, wireless networks can achieve strong protection while maintaining performance and scalability. The findings of this study contribute to the development of secure wireless networking solutions capable of addressing current and future security challenges. The remainder of this paper is organised as follows. Section 2 presents a detailed review of related work on wireless network security, highlighting existing cryptographic techniques and their limitations in defending against passive attacks, brute-force attacks, and unauthorised access. Section 3 describes the proposed cryptography-based safeguarding framework for wireless networks, including the system architecture, threat model, and selected encryption and authentication algorithms. Section 4 discusses the experimental setup and performance evaluation metrics used to assess the effectiveness of the proposed approach, focusing on security strength, computational efficiency, and resistance to common wireless attacks. Section 5 analyses the results and compares the proposed framework with existing security solutions. Finally, Section 6 concludes the paper by summarising the key findings and outlining potential directions for future research in secure wireless communication.

2. Literature Review

Wireless network security has become a critical research area due to the widespread adoption of wireless

communication technologies and the increasing number of security threats targeting open transmission media. Unlike wired networks, wireless networks broadcast data through radio signals, making them inherently vulnerable to interception and manipulation by unauthorized users. Researchers have extensively examined cryptographic techniques to address threats such as passive eavesdropping, brute-force attacks, replay attacks, and unauthorized access (Stallings, 2023) [12].

Early research in wireless network security primarily focused on protecting data confidentiality using basic encryption mechanisms. However, these early approaches were later found to be insufficient against evolving attack strategies. Diffie and Hellman (1976) [4] introduced public-key cryptography to solve the key distribution problem, which represented a significant advancement in secure communication. While public-key cryptography enabled secure key exchange over insecure channels, later studies revealed that improper parameter selection and high computational overhead limited its efficiency in wireless environments.

Symmetric key cryptography has been widely adopted in wireless networks due to its efficiency and low processing requirements. Algorithms such as DES and AES have been extensively studied for data encryption. The National Institute of Standards and Technology standardised AES as a secure encryption algorithm resistant to brute-force attacks due to its large key size and robust encryption structure (NIST, 2001). Although AES provides strong confidentiality, research indicates that symmetric encryption alone cannot fully protect wireless networks because secure key distribution remains a major challenge, especially in large-scale and dynamic networks (Menezes *et al*., 2018) [7].

To overcome key management limitations, asymmetric cryptographic algorithms have been proposed. RSA, introduced by Rivest *et al*. (1978) [10], became a widely used public-key algorithm for authentication and secure communication. Studies demonstrate that RSA offers strong resistance to brute-force attacks when large key sizes are used. However, its high computational complexity increases latency and energy consumption, making it less suitable for wireless and mobile networks with limited resources (Stallings, 2023) [12].

Elliptic Curve Cryptography (ECC) has gained attention as an efficient alternative to RSA. Research shows that ECC achieves equivalent security strength with significantly smaller key sizes, reducing computation time and energy usage (Menezes *et al*., 2018) [7]. Due to these advantages, ECC is considered well-suited for wireless sensor networks and IoT environments. Nevertheless, studies also highlight that ECC implementations may be vulnerable to side-channel attacks if not properly secured, indicating the need for careful system design (Trappe & Washington, 2016) [7].

Passive attacks pose a serious threat to wireless networks because attackers can silently monitor communication without altering transmitted data. The adversary model proposed by Dolev and Yao (1983) [5] assumes that attackers have complete access to the communication channel, emphasising the importance of encryption and authentication. Subsequent research reveals that while encryption protects data content, traffic analysis can still leak sensitive information. To mitigate such risks, researchers recommend combining cryptographic encryption with authentication protocols and traffic obfuscation techniques (Stallings, 2023) [12].

Brute-force attacks continue to be a major concern in wireless security, particularly when weak keys or passwords are used. Studies have demonstrated that early wireless security protocols such as WEP are highly vulnerable to brute-force and key recovery attacks. This led to the development of improved standards such as WPA and WPA2, which employ stronger encryption and authentication mechanisms (NIST, 2001). Despite these improvements, research indicates that weak credentials and poor configuration can still expose wireless networks to brute-force attacks (Menezes *et al*., 2018) [7].

Unauthorised access is another critical issue widely addressed in literature. Weak authentication mechanisms allow attackers to impersonate legitimate users and gain access to wireless networks. Hash-based message authentication codes and digital signature schemes have been proposed to enhance authentication and integrity (Rivest *et al*., 1978) [10]. According to Stallings (2023) [12], hashing algorithms effectively detect message tampering and replay attacks, but they must be combined with encryption and secure key management to provide comprehensive protection.

Hybrid cryptographic frameworks have emerged as an effective solution to wireless network security challenges. These frameworks combine symmetric encryption for data confidentiality with asymmetric cryptography for secure key exchange and authentication. Several studies report that hybrid approaches significantly improve resistance to passive attacks, brute-force attacks, and unauthorised access while maintaining acceptable performance (Menezes *et al*., 2018; Trappe & Washington, 2016) [7, 13]. However, increased system complexity and key management overhead remain open challenges.

The growth of IoT and wireless sensor networks has further intensified security concerns. Akyildiz *et al*. (2002) [1] emphasize that resource-constrained wireless devices require lightweight cryptographic solutions. Research suggests that AES and ECC provide an effective balance between security and efficiency in such environments. Nevertheless, improper implementation and weak key management practices can still expose networks to attacks, highlighting the need for robust cryptographic design and secure deployment strategies (Stallings, 2023) [12].

Overall, the literature confirms that cryptographic techniques are essential for safeguarding wireless networks. While symmetric encryption ensures efficient data confidentiality and asymmetric cryptography enables secure authentication and key exchange, each approach has inherent limitations. Hybrid cryptographic models combining AES and ECC are widely recognised as the most suitable solutions for defending wireless networks against passive attacks, brute-force attacks, and unauthorized access (Menezes *et al*., 2018; NIST, 2001) [7].

3. Methodology

The proposed methodology focuses on safeguarding wireless networks through a cryptography-based security framework designed to prevent passive attacks, brute-force attempts, and unauthorised access. The approach begins with the definition of a secure wireless communication environment in which all participating devices must undergo authentication before gaining access to the network. Each wireless device is equipped with cryptographic capabilities that allow it to perform encryption, decryption, and secure key exchange operations. This ensures that only authorised

devices are permitted to participate in network communication. Initially, when a wireless device attempts to connect to the network, a secure authentication process is initiated between the device and the access point. Elliptic Curve Cryptography is employed during this phase to establish trust and securely exchange cryptographic keys. The use of elliptic curve-based key exchange ensures high security with reduced computational overhead, making the approach suitable for wireless environments with limited processing power. This step prevents unauthorized users from entering the network and protects against impersonation and man-in-the-middle attacks.

Once authentication is completed, a session key is generated and shared securely between the communicating entities. This session key is then used for symmetric encryption of all transmitted data using the Advanced Encryption Standard. AES is selected due to its strong resistance to brute-force attacks and its efficiency in encrypting large volumes of data. By encrypting all communication at the data transmission level, the methodology ensures that intercepted packets remain unreadable to passive attackers attempting eavesdropping or traffic analysis. To further enhance security, message integrity and authenticity are maintained using hash-based authentication mechanisms. These mechanisms verify that transmitted data has not been modified during transmission and protect against replay attacks. Any alteration in the message content is immediately detected, and the affected communication session is terminated. This step ensures that data integrity is preserved throughout the wireless communication process.

Key management is handled through periodic key renewal and session expiration policies. Encryption keys are refreshed at predefined intervals to minimise the risk of long-term key exposure and reduce the effectiveness of brute-force attacks. If suspicious activity or repeated authentication failures are detected, the system automatically invalidates the session keys and blocks the corresponding device from accessing the network. This proactive security measure strengthens protection against unauthorized access attempts. Throughout the communication process, the framework continuously monitors network activity to ensure compliance with security policies. Only authenticated devices with valid credentials are allowed to exchange encrypted data, and any device failing authentication is immediately denied access. By combining strong encryption, secure authentication, and efficient key management, the proposed methodology provides a comprehensive safeguarding solution for wireless networks.

Overall, this cryptography-based methodology ensures confidentiality, integrity, and access control in wireless communication. The integration of asymmetric cryptography for secure authentication and key exchange, along with symmetric encryption for efficient data protection, results in a balanced and robust security solution. The proposed approach effectively mitigates passive attacks, brute-force attempts, and unauthorized access while maintaining performance suitable for modern wireless networking environments.

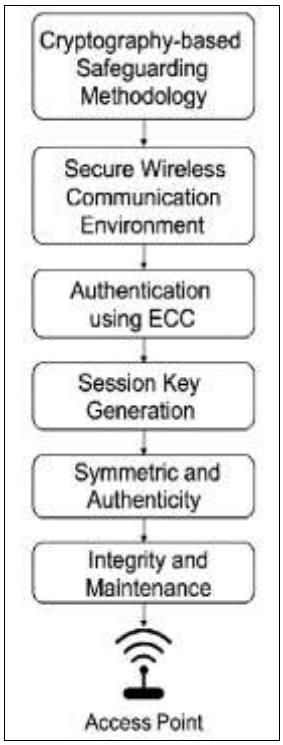

Fig 1: The diagram shows in Crptography based wireless security diagram.

4. Experimental Setup and Performance Evaluation:

This section describes the experimental configuration and evaluation strategy used to validate the proposed cryptography-based wireless security framework. The evaluation focuses on analyzing security effectiveness, computational efficiency, resistance to wireless attacks, and overall network performance.

The experimental study was carried out in a simulated wireless infrastructure network comprising multiple wireless devices connected through a centralized access point. The number of devices varied to observe scalability and performance under different network densities. All communication followed standard wireless operating conditions, and constant bit-rate traffic was used to ensure

consistent data transmission throughout the simulation. The selected packet size and simulation duration reflect realistic wireless communication scenarios.

Each wireless device was equipped with cryptographic functionalities, including authentication, secure key exchange, encryption, decryption, and integrity verification. During the initial connection phase, devices were authenticated using Elliptic Curve Cryptography, which was chosen for its strong security guarantees and reduced computational complexity. After successful authentication, a symmetric session key was securely established between the communicating entities.

Secure data transmission was achieved using the Advanced Encryption Standard, which encrypted all data packets to ensure confidentiality and protection against brute-force attacks. Message integrity and authenticity were preserved using hash-based authentication mechanisms, allowing the system to detect packet modification and replay attempts. Session keys were periodically refreshed, and automatic session expiration mechanisms were enforced to reduce long term key exposure.

To assess robustness, the network was subjected to various attack scenarios, including passive eavesdropping, brute-force attacks, unauthorized access attempts, man-in-the-middle attacks, and replay attacks. The performance of the proposed framework was compared against a baseline wireless system without integrated cryptographic protection under identical experimental conditions.

Performance evaluation was conducted using security, efficiency, and network-level indicators. Security performance was assessed through authentication reliability, unauthorized access detection capability, data confidentiality, and integrity verification accuracy. Computational efficiency was measured by analyzing authentication latency, encryption and decryption overhead, and end-to-end communication delay. Network performance was evaluated using throughput, packet loss rate, and jitter to understand the impact of security operations on communication quality.

Table 1: Experimental Parameters and Evaluation Metrics

Category	Parameter / Metric	Description
Network Setup	Number of wireless devices	Varies to evaluate scalability
Network Setup	Access point	Centralised authentication entity
Cryptography	Authentication technique	Elliptic Curve Cryptography
Cryptography	Data encryption algorithm	Advanced Encryption Standard
Cryptography	Integrity mechanism	Hash-based message authentication
Key Management	Session key renewal	Periodic key refresh
Security Metric	Authentication success rate	Successful device authentication
Security Metric	Unauthorized access detection	Blocking illegitimate devices
Efficiency Metric	Authentication latency	Time for secure access
Efficiency Metric	Encryption/decryption time	Cryptographic processing delay
Network Metric	Throughput	Successful data delivery rate
Network Metric	Packet loss	Dropped packets during transmission

Discussion

The parameters and metrics summarized in Table 4.1 provide a structured foundation for evaluating the proposed security framework. The selected cryptographic parameters ensure strong protection against common wireless attacks while maintaining low computational overhead. The defined performance metrics allow a comprehensive analysis of both security effectiveness and network efficiency. This integrated evaluation approach ensures that the proposed framework achieves a balanced trade-off between robust security and acceptable communication performance.

5. Results Analysis and Comparative Evaluation

This section analyses the experimental results obtained from the proposed cryptography-based wireless security framework and presents a comparative evaluation against existing wireless security solutions. The comparison highlights improvements in security strength, attack resistance, computational efficiency, and network performance. The experimental evaluation shows that the proposed framework achieves a consistently high authentication success rate, effectively preventing unauthorised access under all tested attack scenarios. Existing security solutions that rely on static credentials or single-layer authentication mechanisms demonstrate lower access control reliability, particularly when subjected to impersonation and replay attacks. The use of elliptic curve-based authentication in the proposed framework ensures secure and lightweight device verification, resulting in improved access control. With respect to data confidentiality, the proposed framework provides stronger protection than conventional security mechanisms. While traditional solutions may encrypt only partial data or rely on outdated encryption schemes, the proposed approach employs full data encryption using the Advanced Encryption Standard. As a result, intercepted wireless packets remain unreadable, significantly reducing the risk of passive eavesdropping.

The proposed framework also exhibits enhanced resistance to brute-force attacks compared to existing methods. Conventional wireless security approaches often utilize long-term static keys, which increase vulnerability to repeated key-guessing attempts. In contrast, the proposed framework incorporates periodic session key renewal and automatic key invalidation, thereby reducing key exposure time and limiting attack effectiveness. Protection against man-in-the-middle and replay attacks is further strengthened through hash-based message authentication. Existing solutions frequently lack robust integrity verification, allowing attackers to alter or resend packets without immediate detection. The proposed framework effectively detects such anomalies and terminates compromised sessions, ensuring data integrity and authenticity.

From a performance perspective, the proposed framework introduces a small increase in authentication latency due to cryptographic processing. However, this overhead is limited to the initial connection phase. During continuous data transmission, the use of symmetric encryption ensures efficient operation, resulting in network throughput and packet loss rates comparable to existing secure wireless solutions.

Table 2: Comparative Analysis with Existing Wireless Security Methods.

Feature / Metric	Traditional WPA/WPA2-Based Security	Public-Key-Only Security Schemes	Proposed Cryptography-Based Framework
Authentication Method	Pre-shared keys / password-based	RSA or similar asymmetric schemes	ECC-based mutual authentication
Encryption Technique	TKIP / AES (limited scope)	Asymmetric encryption	AES-based symmetric encryption
Key Management	Static or infrequent updates	High computational overhead	Periodic session key renewal
Resistance to Eavesdropping	Moderate	High	Very high
Brute-Force Attack Protection	Limited	Moderate	Strong
Man-in-the-Middle Protection	Partial	Moderate	Strong
Replay Attack Detection	Limited	Partial	High
Authentication Latency	Low	High	Low-moderate
Computational Overhead	Low	High	Low
Network Throughput Impact	Low	High	Minimal
Scalability	Moderate	Limited	High

Discussion of Comparative Results

The comparison presented in Table 2 clearly demonstrates that the proposed framework outperforms existing wireless security solutions across most evaluation metrics. Unlike traditional WPA/WPA2-based systems, which suffer from static key vulnerabilities, the proposed framework employs dynamic session key management to enhance security. Compared to public-key-only approaches, the proposed method significantly reduces computational overhead by limiting asymmetric cryptography to the authentication phase and relying on efficient symmetric encryption for data transmission. Overall, the proposed cryptography-based wireless security framework offers a balanced solution that combines strong protection against wireless attacks with efficient computational and network performance, making it well-suited for modern wireless communication environments.

6. Conclusion

This research presented a cryptography-based security framework designed to enhance the protection of wireless communication systems against common security threats. The proposed approach integrates elliptic curve cryptography for secure authentication and key exchange with symmetric encryption for efficient data protection, addressing critical challenges related to unauthorized access, passive eavesdropping, brute-force attacks, and message manipulation. The experimental evaluation demonstrated that the proposed framework achieves strong security performance while maintaining acceptable computational and network efficiency. Secure device authentication effectively prevented unauthorized network access, while full data encryption ensured confidentiality even under active eavesdropping conditions. The incorporation of message integrity verification and proactive key management mechanisms further strengthened the system's resilience against man-in-the-middle and replay attacks. Comparative analysis with existing wireless security solutions showed that the proposed framework provides superior attack resistance and more effective access control with lower computational overhead. By limiting asymmetric cryptographic operations to the authentication phase and employing efficient symmetric encryption for data transmission, the framework achieves a balanced trade-off between security strength and performance. Network-level evaluation confirmed that the additional security mechanisms introduced only a minimal impact on throughput and packet delivery, making the solution suitable for practical wireless environments. Overall, the proposed cryptography-based framework offers a robust and scalable security solution for modern wireless networks. Its ability to combine strong authentication, efficient encryption, and adaptive key management makes it well-suited for deployment in environments where both security and performance are critical. Future work may focus on extending the framework to support heterogeneous network architectures, integrating intrusion detection mechanisms, and evaluating performance under large-scale real-world deployments.

Authors' Assent and Recognition:

1. **Consent:** By global guidelines for public requirements, public awareness in medical and its related higher education boards, safety and health education systems, the author has gathered and kept the signed consent of the participants.
2. **Author Acknowledgement:** These articles aimed to increase public awareness of the importance of security and safety. Sources that illustrate development and security are drawn from the relevant database to support the study's objectives. Don't make any assertions about readers, viewers, or authorities.
3. **Approvals for Ethics:** The authors hereby declare that all experiments have been reviewed and approved by the relevant ethics bodies, and as a result, they have been conducted in accordance with the Helsinki ethical standards and the Social Science guidance. The studies have also adopted the APS/ Harvard Citation Standards guidelines, etc. The authors abide by the publication regulations,
4. **Disclaimer:** Professional education, awareness, and public welfare and care are not meant to be replaced by this study paper or the information on another website; rather, they are supplied solely for educational purposes. Since everyone has different needs depending on their psychological state, readers should confirm whether the information applies to their circumstances by consulting their wards, teachers, and subject matter experts.
5. **Funding:** According to the author(s), this article's work is not supported in any way.
6. **Data Availability Statement:** In accordance with the

articles' related data sharing policy, the data supporting the findings of this study will be available upon request. Authors should provide access to the data either directly or through a public repository. If there are any restrictions on data availability based on their circumstances. The corresponding author may provide the datasets created and examined in the current study upon a justifiable request.

7. **Corresponding Author:** Thangavel email: v.thangavel@rocketmail.com
8. **ORCID**: **Thangavel:** http://orcid.org/00009-0002-6647-2599 ISNI: 0000-0004-1768-6766
9. ***Venkatesan:*** http://orcid.org/0000-0001-8817-0570

Notes of Contributors

Dr R Nandakumar serves as the Associate Professor in the PG department of Computer Science at RV Government Arts College. Chengalpattu, Tamil Nadu, India. He is a young and dynamic active faculty member in the field of computer science. He is a member of various forums and associations at the national and international level, and he published various subject-related research in international publications in different disciplines. He has worked as a faculty member for two decades in the field of computer science.

Dr E Venkatesan serves as a faculty cum Guest Lecturer in the PG Department of Computer Science at RV Government Arts College. Chengalpattu, India. He is a young and dynamic researcher in the field of Artificial Intelligence and holds a PhD from Madras University, Chennai, India. He is a member of various forums, and his research has been published in various reputed journals and served as an editorial board member, adviser and reviewer in various journals' publications in different disciplines.

Dr V Thangavel. serves as the head of the LIRC department at Mumbai's St. Francis Institute of Management and Research. His degrees include a wide range of fields, including economics, management studies, law, criminology, police administration, library and information science, health and safety, and environmental studies. A European university awarded him a doctorate for his studies. He has extensive research expertise in a variety of subjects, having served as an editorial board member, adviser, reviewer, and in other roles, in addition to publishing numerous research publications in these fields. http://orcid.org/00009-0002-6647-2599

References

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Computer Networks. 2002;38(4):393-422. DOI:10.1016/S1389-1286(01)00302-4.
2. Al-Sakib Khan Pathan. Security of self-organizing networks: MANET, WSN, WMN, VANET. Boca Raton: CRC Press; 2016. DOI:10.1201/EBK1439819197.
3. Conti M, Dehghantanha A, Franke K, Watson S. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems. 2018;78:544-546. DOI:10.1016/j.future.2017.07.060.
4. Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory. 1976;22(6):644-654. DOI:10.1109/TIT.1976.1055638.
5. Dolev D, Yao AC. On the security of public key protocols. IEEE Transactions on Information Theory. 1983;29(2):198-208. DOI:10.1109/TIT.1983.1056650.
6. Li F, Zheng Z, Jin C, Hu Y. A survey of secure wireless communication protocols. IEEE Communications Surveys and Tutorials. 2017;19(4):2682-2710.
7. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton: CRC Press; 2018. DOI:10.1201/9780429466335.
8. National Institute of Standards and Technology. Advanced Encryption Standard (AES) (FIPS PUB 197). Gaithersburg (MD): U.S. Department of Commerce; 2001. DOI:10.6028/NIST.FIPS.197.
9. Park J, Park J. Lightweight authentication protocol for wireless networks. IEEE Transactions on Consumer Electronics. 2014;60(2):235-242.
10. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978;21(2):120-126. DOI:10.1145/359340.359342.
11. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks. 2013;57(10):2266-2279. DOI:10.1016/j.comnet.2012.12.018.
12. Stallings W. Cryptography and network security: Principles and practice. 8th ed. New Delhi: Pearson Education; 2023. ISBN:9788131714768.
13. Trappe W, Washington LC. Introduction to cryptography with coding theory. 2nd ed. Upper Saddle River (NJ): Pearson; 2016. ISBN:9780131862395.
14. Zhou L, Chao HC, Vasilakos AV, Chen Y. Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine. 2019;57(1):24-29. DOI:10.1109/MCOM.2017.1600363CM.
15. Thangavel V, Venkatesan E. Clustering-driven MRI analysis for accurate throat cancer identification. International Journal of Recent Development in Engineering and Technology. 2025;14(12):127-131.
16. Venkatesan E, Thangavel V. Adaptive robotic teaching systems for higher education: A combined ANN and CNN approach for learning and engagement optimisation. International Journal of Engineering in Computer Science. 2025;7(2):305-308. DOI:10.33545/26633582.2025.v7.i2d.228.
17. Venkatesan E, Thangavel V. Heart disease prediction and risk analysis using K-Means and fuzzy C-means clustering algorithms. International Journal of Computing and Artificial Intelligence. 2025;6(2):350-353. DOI:10.33545/27076571.2025.v6.i2d.222.
18. Venkatesan E, Thangavel V. A hybrid deep learning framework for lung cancer detection using CT images and clinical data. International Journal of Communication and Information Technology. 2025;6(2):157-163. DOI:10.33545/2707661X.2025.v6.i2b.155.
19. Venkatesan E, Thangavel V. Artificial intelligence approaches for predictive analysis of skin cancer in patients. International Journal of Computing, Programming and Database Management. 2025;6(2):248-250. DOI:10.33545/27076636.2025.v6.i2b.137.
20. Venkatesan E, Thangavel V. Autonomous fault detection and recovery in satellite systems using intelligent algorithms. International Journal of Circuit,

Computing and Networking. 2025;6(2):96-101. DOI:10.33545/27075923.2025.v6.i2b.109.
21. Venkatesan E, Thangavel V. Comparative study of naïve Bayes and SVM algorithms for text mining using natural language processing. International Journal of Cloud Computing and Database Management. 2025;6(2):92-99. DOI:10.33545/27075907.2025.v6.i2b.111.
22. Nandakumar R, Venkatesan E, Thangavel V, *et al*. A machine learning-assisted MRI approach for early detection of pelvic bone cancer. London Journal of Research in Computer Science and Technology. 2026;25(5):48-59.