American Academic Scientific Research Journal for Engineering, Technology, and Sciences

ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

https://asrjetsjournal.org/index.php/American_Scientific_Journal/index

A Review of the Effectiveness of Symmetric and Asymmetric Cryptography Methods with Multi-Level Key Management in Wireless Networks

Rana Khalid Sabri[a]*, Hiba Abdulkareem Saleh[b], Omar Ibrahim Alsaif [c]

[a]Department of Cybersecurity Engineering and Cloud Computing Technologies, Technical Engineering College for Computer and AI, Northern Technical University, Mosul, Iraq

[b]Department of Chemical and Petroleum Industries Techniques Engineering, Technical Engineering College, Northern Technical University, Mosul, Iraq

[c]Polytechnique College/Mosul, Northern Technical University, Mosul, Iraq

[a]Email:rana.khalids@ntu.edu.iq

[b]Email:hiba.abdlkareem@ntu.edu.iq

[c]Email:omar.alsaif@ntu.edu.iq

Abstract

Wireless networks have nearly no limitations when it comes to communication systems powered by electricity, which are growing all over the globe. However, it is essential to implement robust security measures as sophisticated cyber attacks evolve. The study mainly focuses on symmetric and asymmetric key cryptography, especially their efficiency. The suggested system makes key distribution easy by not only eliminating complicated setups but also employing a secure photon recorder and strict communication protocols. The research combines theoretical analysis and practical simulations to prove the applicability of the proposed method and to determine its effectiveness in maintaining mobile network environments with high security. Moreover, the technique is adaptable to the demanding constraints of modern wireless communication systems with little difficulty. Moreover, the paper includes a detailed comparison of the existing solutions and a set of future research directions to effectively overcome the current barriers related to key management schemes in the area. The main objective is to enable the wireless domain to have a more efficient, scalable, and secure infrastructure.

Keywords: Key management; Multi-level; Wireless; Security; Encryption.

Received: 10/3/2025
Accepted: 12/3/2025
Published: 12/13/2025

** Corresponding author.*

1. Introduction

Remote communication technology has also posed a variety of security problems. The wireless network security main difficulties are based on the unpredictability of the communication channel. In the case of wireless technology, the performance and efficiency of the coming technology revolution are already seen with the great leaps taken already [1]. It has mainly security on the upper layers of the network communication that it is working on heavily. The adoption of wireless technology has not yet happened completely as there is not a sound security structure that monitors and secures its use, thus allowing various threats to exist [1]. The Sixth Generation (6G) Communication Networks aim at nothing less than the transformation of the data transmission speed and connections to be so smooth that 6G would be a quickly perfecting worldwide phenomenon [2]. These next-generation networks are expected to operate on sub-THz frequency bands, enabling unprecedented performance and efficiency [2]. However, these new technologies require network security to defend against new threats, protect sensitive information, and ensure the safekeeping of communications in these new systems [3]. Cryptography is widely as an effective security solution in distributed computing, as it safeguards sensitive information accessed by potential cyberattacks [4]. Various research studies have introduced solutions to enhance the security of wireless networks at the data link and network layers. Two main cryptography systems are used today: symmetric systems called also systems with a secret key, and public-key systems [5]. Key management is regarded as one of the significant challenges in network security, as communicating entities must handle multiple cryptographic keys when maintaining secure communication with several parties [6]. A single-level key management system maintains and updates a fixed number of keys across the communication network. Though this application is well-executed, it tends not to be cost-effective and is less valuable in complex and large-scale networks [7]. This paper explores the comparative effectiveness of recent research on securing wireless communication. In peer-to-peer networks, a multi-level key management system ensures secure communication. This is done by applying cryptographic primitives that cocoon a complicated key structure under the simper and weaker keys used in lower layers, which results in better efficiency and improved security [8]. The extra queue added in the message flow is capable of simplifying the system while guaranteeing that just the appropriate messages are there in the network and it also offers a network-centric solution that takes care of key Management schemes (KMS) without the requirement of end-to-end encryption [30]. This leads to a situation where communication is fast and multicast security is created through a very small delay even at sub-nanosecond speeds. Furthermore, the latest multi-level key management algorithms are also presented in the paper, which are already widely applied in cryptographic solutions [31]. In addition, it delves into the difficulties of designing deferred key cascades, proceeding to summarize the study's goals, objectives, and key contributions [8]. Wireless networks face the problem of having to comply with very strict security requirements, especially in high-risk areas like military and medical communication systems. Multi-level security is usually implemented in these systems enabling the access of different information by people according to their classification and signality [9]. Symmetric key management is praised for its simplicity and high efficiency, but still, it is accompanied by some drawbacks such as the problems of secure key distribution and the limitation of the bandwidth that is necessary for this operation. Because of these drawbacks, private key management solutions are continually suggested either as separate solutions or in conjunction with symmetric encryption [32]. In the case of public key management, it is absolutely essential to have a proper understanding of the key distribution which signifies the distribution of these keys within the network. It plays a vital role in ensuring the security of the network by lessening the impact of threats that can arise such as unauthorized key generation, key escalation, and key imports, among others, thus, aiming at the creation of a more secure and scalable cryptographic system [10]. Nonetheless, the establishment of these multi-level applicable cryptographic techniques in the communication of data would help along with creating high-performance access control to simultaneously safeguard sensitive information from the adversaries' eyes. The reason for this is that cryptography is always on the side of secure and reliable communication by keeping the detection, repetition, or access to keys occluded [11]. The use of multi-level security in cryptography not only strengthens the security but also provides a range of efficiencies such as lower costs and shorter times. Better performance from employing such systems can be viewed as organizational performance with reduced operational expenses due to the efficiency gained. Cryptographic Multi-Level Key Management (MKM) is a technique that allows the generation, management, and distribution of cryptographic keys in a secure manner across wireless networks. Key management at the geometric or network or link/MAC layer has traditionally been centralized or attached to the network because of the complexities/risks surrounding security. The separation and expansion of key generation and distribution across multiple layers can increase security drastically, making key management systems more resilient against attacks [12,13]. In comparison, single-layer key management refers to generating and distributing cryptographic keys only in a specific communication layer. Every layer either encrypts and secures data streams at that level or passes them on securely to adjacent layers, making a structured approach to protection [14]. In this approach, the selected layer generates, manages, and distributes cryptographic keys to devices or other layers requiring security. Single-link key management systems typically handle only a specific subset of communications and are often time-limited. The cryptographic keys generated and distributed in this case are only applicable to a given session or connection, and they are typically used to address short-term security requirements [15]. A multi-level Key management system for wireless and mobile networks is introduced by using the Diffie-Hellman algorithm to have a secure key distribution among the network nodes effectively. The difference in this approach is that an advanced encrypted photon recorder is used to improve the key security. Furthermore, the proposed scheme includes an effective and safe communication process with a strong protocol that guarantees the highest security level [16]. The theory is proven by a software security testing and a practical implementation plan for a comprehensive overall comprehension. This makes its accuracy and development well appropriate to the operational setting [17]. The proposed method streamlines deployment by goal-oriented provisioning of cryptographic keys and associations rather than the cumbersome setup process between any two network nodes. The experimental and simulations works shows its practicability on large scale and in real life Reference [18]. In conclusion, this multi-tiered key management scheme provides a new one that is both secure and practical in distributing a key in a wireless/mobile network. The scheme creates a secure environment in which secret cryptographic data is safely secured against unauthorized access or theft. Detailed analysis and numerical simulations have shown that this method is robust and reliable, and it is suitable for practical implementation [1,19].

2. Related Work

In 2019, S.V. Manikanthan and T. Padmapriya [20] proposed the MLKM protocol. The goals of MLKM (Multi-Level Key Management) are reducing the communication overhead, enhancing the detection accuracy, lessening the key memory consumption, and extending the network lifetime. MEHM is not concern for security, resistance to node attack and communication between a clustered Wireless sensor network (WSN) at the other hand, MSKM (Multi-Secret Key Management) focused on security resistance to node attack and communication for clustered WSNIn 2020, A. F. M. Suaib Akhter, and his colleagues [21] investigated different technologies and protocols to increase the security and authentication in VANETs such as Vehicular Ad Hoc Networks. The most fun part has been the multi-layer blockchain. In a wild enough architecture, the GAC controlled the storage of a vehicle's data. LACs Specialized buildings (LACs) check locally according to type of Vehicle using a regional blockchain (LABC). Signed messages were secured using RSA-1024 digital signature model. The research additionally maintained the integrity of the data with the adoption of a digital signature, not allowing data tampering while transmitting the data. Results were stringently protected by encrypt transmission of the messages to avoid unauthorized access to the sensitive content. Vehicle identity was well-controlled by saving it as a public key in the vehicle's local blockchain, while the real identity was safely hidden in LACs to achieve the privacy protection.In 2021, Miss Pritilata and his colleagues [22] suggested a hybrid cryptographic algorithm amalgamating three different methods: multi-prime RSA, DES, and Vernam Cipher-for strengthening the security of data. Multi-prime RSA involves the use of more than two prime numbers in the generation of keys and the processes of encryption and decryption, resulting in better computational efficiency than the former RSA. DES is an encryption method that used a symmetric key to encrypt 64-bit data blocks; however, the short length of the key-56 bits-made it less secure from attacks by now present-day algorithms, such as AES. The Vernam Cipher is a stream cipher that produces ciphertext by combining the plaintext with a random key of the same length using the XOR operation.In 2021, Hakeem and his colleagues [23] continued the research on enhancing LoRaWAN security and used hash chain-based protocols to create unique session keys. These keys, encrypted using salt, helped in protecting attacks that were physical in nature. An AES-based encryption protocol was then selected for message integrity (AES-128-CMAC) and encryption (AES-128-CTR). Hence, the security of LoRaWAN was improved by perfect forward secrecy, protecting against replay attacks using the timestamp, and allowing for periodic key changes to overcome the disadvantage of using static keys in conventional LoRaWAN implementations. Simulations proved that the protocol was more efficient when reducing transmission time, energy consumption, and computation overhead, making it apt for resource-constrained IoT devices.In 2021, Sanjeev Kumar and his colleagues [24] Their research "A Novel Approach of Symmetric Key Cryptography" proposed a new method to enhance data security using symmetric encryption. The Caesar Cipher was augmented from the proposed study (which represents the third contribution) in the sense that the mechanism to derive the symmetric encryption key was a hash code, and only the hash code and length, not the key itself, passed on to the receiver as it made the transmission process more reliable. You can encrypt your password using letters uppercase and lowercase—numbers, and special symbols. This is simple and effective, and it can be implemented in a few math calculations and can be helpful in many domains. It also improves secure transmission by sending only the hash code and the key length, providing additional protection during data transmission over the network. In 2022, Kokab Havashemi Rezaeipour and Hamid Barati[25]. Proposed a hierarchical key management technique for wireless sensor networks. Their approach involves dividing the network into multiple zones, each managed by a zone manager with higher processing power and memory capacity. The system employs three types of keys:

- Public Key: The base station secures communication with the nodes.

- Communication Key: Ensures secure channels for zone managers and base station communication

- Zone Key: Uses secure communication within each zone

The authentication mechanism of the system depends on a physical identifier (MAC address) as well as a secret key, thus providing strong protection against attacks. In 2022, Hua Yi Lin and his colleagues [1] introduced a hierarchical security architecture employing M-tree-based ECDSA (Elliptic Curve Digital Signature Algorithm). It provides the possibility for the key management to be dynamic and is able to react on topological change of the IoV ecosystem and, accordingly, the simple security schema can adopt to the structure of the overall system. This reduces the number of steps needed to resync system keys and shortens the key reconstruction time. Moreover, M-tree key management and reliable data transmission are integrated to ensure data security during communication. This will help in adaptive functioning of the IoV network and real-time data transfer. This multilevel security framework stops unauthorized entities such as drivers, observers, or rogue vehicles from planting and altering critical information. The method uses M-tree structure, ECDSA, and a holistic security framework to secure the communication and data transfer of IoV. Through simulation and analysis, the study proves the efficiency and effectiveness of the featured method in the improvement of security and performance attributes. In 2023, Sahar Ahmadi Khah, and his colleagues [26] elaborate on a multi-level, dynamic key management technique for a WSN where the network is divided into five hierarchical levels with clusters of varying sizes at each level. Four major phases compose the key management process: network leveling, clustering, key establishment (cluster, pairwise, and gateway keys), and rekeying. The suggested approach implements an RC5 (Rivest Cipher 5) algorithm for symmetric encryption together with a MAC-based authentication system which together provide the necessary measures for data security, less power usage, and communication overhead to the least degree possible. The major advantage of this method is that it can be easily scaled and is versatile to establish secure channels even among nodes with limited resources. Lastly, it equally conserves energy, efficiently uses memory, resists node capture attacks to a fair extent, and supports sound rekeying methods to maintain data integrity with forward and backward secrecy. In 2023, Muhaijar and his colleagues [27] presented a hierarchical key management system designed to ensure security for WSNs in medical contexts. The proposed approach employs the HEED protocol (Hybrid Energy-Efficient Distributed Clustering) for clustering, lightweight cryptographic operations, and pseudorandom number generation. The protocol must conserve sensor energy and, at the same time, provide a long life for the network. Encryption used was RC5(Rivest Cipher 5) in Cipher Block Chaining mode to balance the needs of confidentiality, integrity, and authentication with resource consumption. In managing the keys, a Bloom scheme was used to generate and distribute secure keys and derive shared keys from exchanged keys whereby a pseudorandom number generator enhances resistance to attacks [3]. According to results, the perfectly designed novelty outperformed DSKM (Dynamic Secret Key Management) and SSI (Self-Sovereign Identity) techniques concerning energy conservation, memory space used, and scalability, with respect to node capture attacks. WSN communications in medical environments use this system to provide security while balancing light designs and heavy security. In 2024, Asha Rani Mishra. [28] made a case for Elliptic Curve Cryptography (ECC), as the preferred option since it offers high security with low resource consumption due to the small size of its key. ECC has emerged as the more computationally efficient and memory-efficient alternative compared to RSA. Because symmetric algorithms are also resource-efficient, they may provide confidentiality; however, they lack robust authentication and key exchange mechanisms provided by some asymmetric algorithms, such as ECC. With the constrained memory and computational resources fundamental to WSNs, efficient key management assumes major significance. Different approaches were applied to address these limitations, namely pre-distributed keys, cluster-based local key management, and dynamic key updates, which serve to enhance security and scalability. Still, in all these scenarios, WSNs remain in serious danger. The main bottleneck for ECC is the computational limitation that makes its implementation difficult on energy-constrained sensor nodes, as it requires high processing power. Furthermore, these approaches consume a significant amount of energy in key management and authentication processes, which reduces the network's overall lifetime. Louis Frank and his colleagues [29] propose a new approach in 2024 for designing lightweight and efficient cryptographic algorithms for the security of resource-constrained WSNs from a geometric (trigonometric) perspective. From the described methodology, it would ideally place the least load possible on the sensor node resources, sufficiently providing security standards equal to or better than those provided by the existing alternatives. The researchers suggested that the design of TBC (Truncated Binary Coding) would have been rigorously tested via extensive simulations and performance analyses to show its practical application. They also highlighted problems of scalability, resistance to state-of-the-art attacks, and the need for optimization of the algorithms for particular use cases.

3.Methodology

3.1 The Secure Multilevel Key Management (MLKM) Protocol

The protocol is thus structured into three stages, offering one predominant key management paradigm with a few exceptions employing crypto techniques like hashing, homomorphic encryption, dynamic passwords, profile sequences, random numbers, and XOR functions as shown in Figure 1 [19,20].

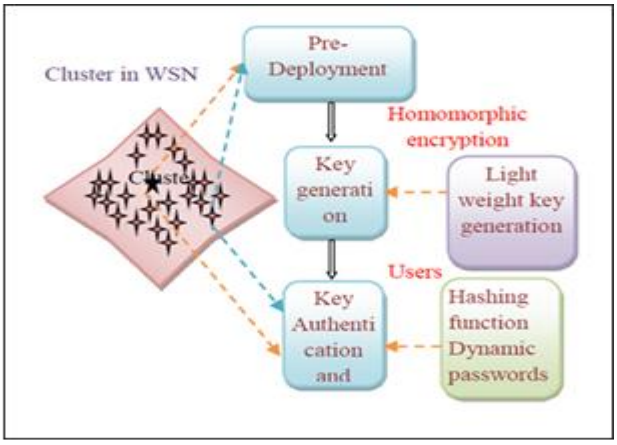

Figure 1: MSKM and MLKM protocol in dynamic cluster base WSN [19,20]

The figure illustrates the two protocols in a dynamic cluster-based Wireless Sensor Network (WSN) context. It provides a brief summary of the three stages of the MSKM (Multi-Secret Key Management) protocol and describes the means and technologies utilized in each stage for communication to be secure.

As shown below:

- Pre-Deployment Phase:

The very first phase of building the network is enabling it to communicate securely. Establish clusters of sensors in WSN that serve as basic building blocks for communication and key management.

- Key Generation Phase:

Keys are generated using homomorphic encryption techniques to ensure security. It enables computations to be performed over encrypted data without needing to decrypt it, thus providing a significant improvement in security and privacy. The protocol also uses the lightweight key generation which is effective for WSN nodes as these nodes have energy and computing limitations due to low processing power.

- Key Authentication and Verification Phase:

Keys generated are authenticated and verified for secure and legitimate communication. It uses the following technique:

- Hashing functions: these will allow you to create unique hash values for your data so it can be verified.

- Time or conditions:(such as the case with dynamic passwords) change, they add another layer of protection against attacks.

- The first property is purpose which helps avoid unauthorized user or device to participate in the communication.

3.2 Blockchain-Based-Privacy-Preserving Authentication System

This system incorporates blockchain technology via a Global Authentication Center (GAC) and Local Authentication Centers (LACs) to secure vehicle data in VANETs (Vehicular Ad Hoc Networks). Digital signatures add an additional layer of security.

- Purpose: Improves the confidentiality, security, and integrity of vehicle communications.

- Visual Aids: These are likely to be the architecture diagrams of the blockchain system showing how the vehicles and the authentication centers interact Figure 2 illustrates the approach that was applied for the tree structure of the proposed blockchain-based-privacy-preserving system authentication in VANETs [21], with a table 1 comparison between four levels for the proposed blockchain.

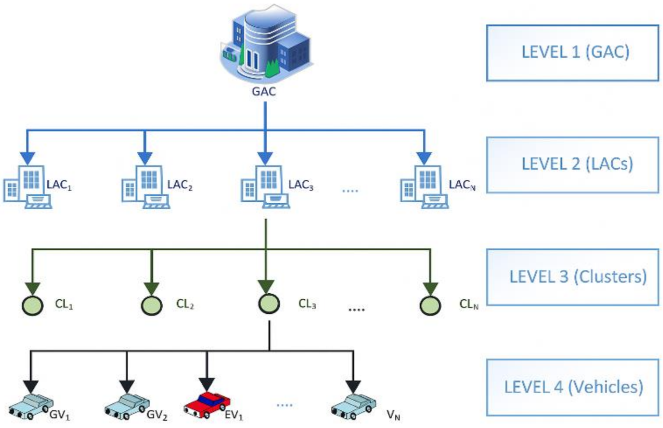

Figure 2: Tree structure of the proposed method [21]

Table 1: A comparison between four levels for the proposed blockchain based privacy preserving authentication system in VANETs

Level	**Component**	**Role**	**Key Functions**
Level 1	Global Authentication Center (GAC)	Top-level authority managing the entire network	- Central hub for overall network management- Maintains the blockchain ledger for secure transaction records- Connects with multiple Local Authentication Centers (LACs)
Level 2	Local Authentication Centers (LACs)	Regional centers handling local vehicle data	- Authenticate vehicles using blockchain and cryptographic techniques- Synchronize with GAC for ledger updates
Level 3	Clusters	Subdivisions under LACs for better vehicle management	- Perform localized authentication for vehicles in their designated area- Enhance scalability and network efficiency
Level 4	Vehicles (GV, EV, VN)	Entities interacting with the system (General, Emergency, Others)	- Secure communication with other vehicles and roadside units- Exchange authenticated traffic data and alerts

3.3 Hybrid Cryptography Algorithm

The proposed solution is centered on a robust layered encryption and decryption mechanism, the one which uses the multi-prime RSA, DES, and Vernam Cipher as its building blocks.

• Objective: It is aimed at providing a stronger data security through combining cryptographic algorithms as a way of securing the data against unauthorized access.

• Visual Aids: A flowchart indicating the progressive steps of the encryption and decryption processes would probably be included in this. The Figure 3 [22].

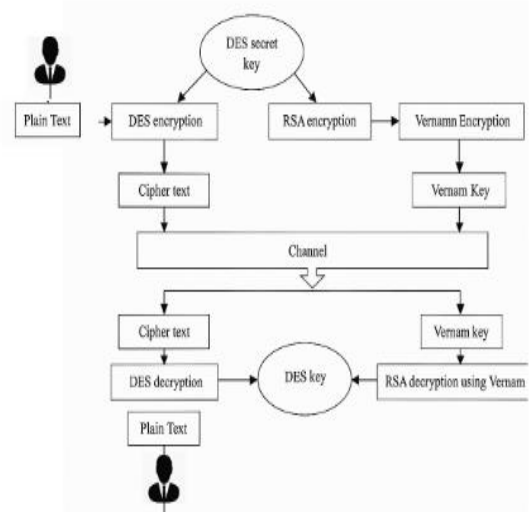

Figure 3: Proposed Multi-Level Algorithm Model

The figure 3 shows in detail the 2 steps **Encryption Process** and **Decryption Process**, the Encryption Process include the data secured using DES encryption which is performed with a key, DES key gets encrypted through the RSA mechanism, the key which is already RSA-encrypted undergoes further encryption with a Vernam key and the ciphertext transmission along with the Vernam-encrypted key is conveyed through the channel. In the Decryption Process include the RSA key is decrypted by using the Vernam key, the DES key is decrypted by the application of the private RSA key and the ciphertext produces original plaintext after going through the decryption process.

3.4. Hierarchical Key Management and Layered Encryption and Decryption Technique

In hierarchical key allocation, keys are managed at different levels, resulting in a high level of security and better control. Layered encryption and decryption are improved by using multiple encryption methods. In efficiency and adaptivity, the system remains efficient and adaptable to different security requirements and threats. There may be diagrams illustrating the hierarchical setup and the responsibilities of the zone managers in key management as shown in Figure (4) [23].

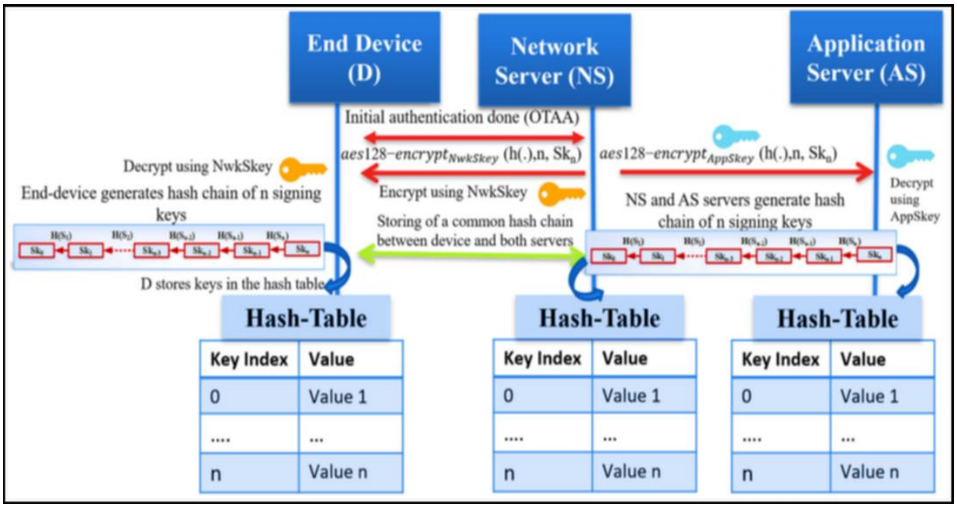
End Device (D)
Network Server (NS)
Application Server (AS)
Initial authentication done (OTAA)
aes128−encrypt_NwkSkey (h(.),n, Skn)
aes128−encrypt_AppSkey (h(.),n, Skn)
Decrypt using NwkSkey
End-device generates hash chain of n signing keys
Encrypt using NwkSkey
Decrypt using AppSkey
NS and AS servers generate hash chain of n signing keys
Storing of a common hash chain between device and both servers
D stores keys in the hash table
Hash-Table
Key Index
Value
0
Value 1
....
...
n
Value n

Figure 4: The overall flowchart of the proposed model [23]

Table 2: compare the methodologies mentioned in this paper

System used	**Advantages**	**Challenges/Limitations**
MSKM and MLKM protocol for key management	Reduced communication costs, improved threat detection accuracy, minimized memory usage, and enhanced energy efficiency.	Complexity in deployment, and reliance on compatibility with existing systems.
Multi-level blockchain system.	Improved identity management, data integrity, and secure communication via blockchain.	High computational overhead, storage challenges, and reliance on high-speed 5G infrastructure.
A hybrid cryptographic algorithm combining multi prime RSA, DES, and Vernam Cipher.	Enhanced encryption efficiency and strong protection using a layered approach.	Increased computational requirements, key management complexity, and implementation challenges in resource-constrained systems.
Hash chain-based protocol for session keys.	Reduced energy consumption, transmission time, and computational overhead, ensuring forward secrecy.	Scalability issues, reliance on a central server, and computational burden from managing hash chains.
Caesar Cipher uses a hash-based key generation mechanism.	Simple implementation, reduced risk of interception, and improved security during transmission.	Increased computational overhead, reliance on hash code security, and slower performance than traditional methods.
A hierarchical key management technique is	Enhanced energy and memory efficiency, strong resistance to	Additional computational load, high expansion costs, and complex

used to divide the network into zones.	replay attacks, and scalability.	dynamic key management.
ECDSA and M-tree structures	Improved dynamic key management, attack resistance, and enhanced real-time secure communication.	High computational complexity in ECDSA and scalability challenges in large-scale networks.
A dynamic and hierarchical key management approach with a multi-level structure.	Reduced energy consumption, improved attack resistance, and enhanced scalability.	Increased system complexity due to multi-level structure and challenges with frequent dynamic rekeying.
Hierarchical key management using HEED and lightweight cryptography.	Strong protection, energy efficiency, and resource optimization.	Difficulty adapting to random sensor distributions and the need for optimization to handle large datasets efficiently.
Elliptic Curve Cryptography (ECC) for efficient key management.	High security with minimal resource consumption, reducing computational overhead.	Computational complexity and increased energy usage from dynamic key management processes.
Trigonometry-Based Cryptography (TBC) for secure WSN communication.	Lightweight cryptographic design providing strong protection with minimal resource use.	Computational complexity, need for real-world testing, scalability issues, and challenges with adapting to more extensive networks.

4. Results Discussions

The choice of the best cryptographic method depends on the specific requirements of the network, such as the security level required, the amount of processing power that can be supported, the factor of energy consumption, and the network architecture. The implementation of ECC in a high-security requirement but limited resources situation is regularly considered due to its high-performance and effectiveness traits. Multi-level key management systems offer a compromise solution, providing robust security whilst dealing with the challenges of complexity and energy efficiency. This condition may fit well with the complex and stratified network structures commonly found in Wireless Sensor Networks (WSNs).

4.1. Network Security

For the technologies in the network security category displayed in Table 1, which provide good protection as well as handle complex security problems they become necessary. Elliptic Curve Cryptography (ECC) is the most secure among all because its strength in cryptography in relation to the key size is very high. Therefore, it is suitable for very strict security needing situations like WSNs, which are limited in both computational resources and battery life. Hierarchical Key Management Method. This method provides very good security for the whole system because of the several thousand keys used and the encryption of the information on many layers of the network, which gives an extra protection against the compromising of nodes and other attacks.

4.2. Resource Usage

The hierarchical Key Management: It was intentionally created to save resources and solve the drawbacks of WSNs in healthcare through applying energy-conscious methods as well as reducing the number of key transfers, which leads to saving sensor power.

4.3. Key Distribution

In hierarchical Key Management Method: It makes key distribution management very easy and fast with its hierarchical structure while reducing the burden on each sensor and at the same time improving the scalability and flexibility of the entire network, also in dynamic and Multi-Level Key Management, the method used here cuts down on communication overhead and power usage by means of a powerful multi-level that is responsive to network variations.

Table 3: compare the methodologies mentioned in this paper

Method	Security	Resource Usage	Key Distribution	Complexity	Cost
ECC for WSNs	High	High efficiency in energy	Not care about distribution	Low	Low
Hierarchical Key Management	Strong	Efficient resource use	High efficiency in key distribution	Medium	Medium
Dynamic and Multi-level Key Management	Medium	Reduces overhead and energy consumption	Supports efficient key revocation and updates	High	High

5 .Conclusion and Future Works

5.1 Conclusion

Various key management techniques have been studied, which are the backbone of the process and the security of the network. A hierarchical key management method is the most accepted among the evaluated methods based on three main factors (security, resource usage, and key distribution). The use of a layered key structure and handling in network zones makes the security very strong. Resource usage is optimized, and the key is effective distribution. It supports applications in most situations, particularly in limited-resource environments like WSNs. The Hierarchical Key Management Method is able to satisfy the requirements of the medical environment and is a strong indicator of its reliability in critical applications where security and reliability of the system are the highest priority. This feature makes the method a serious candidate for securing future network infrastructures that will require efficiency and scalability.

5.2 Future Works

The future investigations will focus on improving the Hierarchical Key Management Method in the following areas: Mobility influence: get a clear understanding of how mobility affects key distribution and security in dynamic networks. Scalability: Adjust the hierarchy according to very high network installations. Advanced cryptography, applies post-quantum cryptography plus AI-improved security. Energy efficiency: Create energy-efficient encryption models for WSNs and IoT applications. Cross-layer Security: implement key management at different network layers to achieve end-to-end security.

References

[1] H. Y. Lin and M.-Y. Hsieh, "A dynamic key management and secure data transfer based on m-tree structure with multi-level security framework for internet of vehicles," *Connection Science*, vol. 34, no. 1, pp. 1089–1118, Dec. 2022, doi: 10.1080/09540091.2022.2045254.

[2] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[3] R. Nazir, A. A. Laghari, K. Kumar, S. David, and M. Ali, "Survey on Wireless Network Security," *Arch Computat Methods Eng*, vol. 29, no. 3, pp. 1591–1610, May 2022, doi: 10.1007/s11831-021-09631-5.

[4] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Netw*, vol. 27, no. 2, pp. 1515–1555, Feb. 2021, doi: 10.1007/s11276-020-02535-5.

[5] S. M. Ali, S. V. Reve, R. Ali, and S. Iqbal, "Key management with cryptography," Accessed: Feb. 10, 2025. [Online]. Available: http://www.computerscijournal.org/dnload/Syed-Minhaj-Ali-Satish-V-Reve-Roohi-Ali-and-Sana-Iqbal-/OJCSV03I02P299-304.pdf

[6] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, p. 102448, 2021.

[7] X. Lin, Y. Pan, W. Feng, H. Zhang, and M. Lin, "MTDB: an LSM-tree-based key-value store using a multi-tree structure to improve read performance," *J Supercomput*, vol. 80, no. 16, pp. 23995–24025, Nov. 2024, doi: 10.1007/s11227-024-06382-5.

[8] S. Bansal and D. Kumar, "IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication," *Int J Wireless Inf Networks*, vol. 27, no. 3, pp. 340–364, Sep. 2020, doi: 10.1007/s10776-020-00483-7.

[9] B. Bhushan and G. Sahoo, "Requirements, Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective," in *Handbook of Computer Networks and Cyber Security*. Cham: Springer, 2020, pp. 683–713, doi: 10.1007/978-3-030-22277-2_27.

[10] P. M. Rao and B. D. Deebak, “A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions,” *Ad Hoc Networks*, vol. 146, p. 103159, 2023.

[11] M. Waqas et al., “The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges,” *Artif Intell Rev*, vol. 55, no. 7, pp. 5215–5261, Oct. 2022, doi: 10.1007/s10462-022-10143-2.

[12] M. Tropea, M. G. Spina, F. De Rango, and A. F. Gentile, “Security in wireless sensor networks: A cryptography performance analysis at MAC layer,” *Future Internet*, vol. 14, no. 5, p. 145, 2022.

[13] P. Anand et al., “IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges,” *IEEE Access*, vol. 8, pp. 168825–168853, 2020.

[14] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, and C. Su, “A physical-layer key generation approach based on received signal strength in smart homes,” *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 4917–4927, 2021.

[15] Y. Cao et al., “The evolution of quantum key distribution networks: On the road to the qinternet,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[16] R. M. Naik, S. V. Sathyanarayana, and T. K. Sowmya, “Key management using elliptic curve Diffie Hellman curve 25519,” in *Proc. 3rd Int. Conf. Multimedia Processing, Communication & Information Technology (MPCIT)*, 2020, pp. 33–39. Accessed: Feb. 10, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9350454/

[17] S. Challa et al., “Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems,” *Future Generation Computer Systems*, vol. 108, pp. 1267–1286, 2020.

[18] Z. Ma et al., “An efficient decentralized key management mechanism for VANET with blockchain,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5836–5849, 2020.

[19] R. V. Saraswathi, L. P. Sree, and K. Anuradha, “Multi-stage key management scheme for cluster-based WSN,” *International Journal of Communication Networks and Information Security*, vol. 10, no. 3, p. 552, 2018.

[20] S. V. Manikanthan and T. Padmapriya, “A secured multi-level key management technique for intensified wireless sensor network,” *Int. J. Recent Technology and Engineering*, vol. 7, 2019.

[21] A. Akhter et al., “A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET,” *Sustainability*, vol. 13, p. 400, 2021. [Online]. Available: https://www.academia.edu/download/77497903/pdf.pdf

[22] Pritilata and Md. A. Mahmood, “Strengthening Data Security Using Multi-level Cryptography Algorithm,” in *Advanced Computational Paradigms and Hybrid Intelligent Computing*, vol. 1373, 2021, pp. 315–324, doi: 10.1007/978-981-16-4369-9_31.

[23] S. A. A. Hakeem, S. M. A. El-Kader, and H. Kim, “A key management protocol based on the hash chain key generation for securing LoRaWAN networks,” *Sensors*, vol. 21, no. 17, p. 5838, 2021, doi: 10.3390/s21175838.

[24] S. Kumar, M. S. Gaur, P. S. Sharma, and D. Munjal, “A novel approach of symmetric key cryptography,” in *Proc. 2nd Int. Conf. Intelligent Engineering and Management (ICIEM)*, 2021, pp. 593–598. Accessed: Feb. 10, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9445343/

[25] H. Barati, “A hierarchical key management method for wireless sensor networks,” *Microprocessors and Microsystems*, vol. 90, p. 104489, 2022.

[26] S. A. Khah, A. Barati, and H. Barati, “A dynamic and multi-level key management method in wireless sensor networks (WSNs),” *Computer Networks*, vol. 236, p. 109997, 2023.

[27] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, “A perfect security key management method for hierarchical wireless sensor networks in medical environments,” *Electronics*, vol. 12, no. 4, p. 1011, 2023. doi: 10.3390/electronics12041011.

[28] A. Mishra, “Elliptic curve cryptography (ECC) for security in wireless sensor network,” 2024. [Online]. Available: https://www.researchgate.net/publication/378239022

[29] L. Frank and E. Louis, “Trigonometry-Based Cryptography for Secure Communication in Wireless Sensor Networks,” *International Journal of Applied Cryptography*, Feb. 2024. [Online]. Available: https://www.researchgate.net/publication/378588155

[30] S. J. Rashid, A. M. Alkababji, and A. M. Khidhir, “Communication and Network Technologies of IoT in Smart Building: A Survey,” *NTU Journal of Engineering and Technology*, vol. 1, no. 1, pp. 1–18, 2021.

[31] S. A. Baker, S. J. Rashid, and O. I. Alsaif, “Fog Computing: A Comprehensive Review of Architectures, Applications, and Security Challenges,” *NTU Journal of Engineering and Technology*, vol. 2, no. 2, pp. 21–28, 2023, doi: 10.56286/ntujet.v2i2.614.

[32] A. A. Ghanim and M. Y. Thanoun, "Wireless Networks Security Flaws and Hacking Avenues of Attacks," *NTU J. Eng. Technol.*, vol. 4, no. 2, pp. 47-53, 2025, doi: 10.56286/ntujet.v4i2.