Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-A, pp. 1117–1130
DOI : 10.47974/JDMSC-2102

Enhancing IoT-based wireless sensor network security with cryptographic techniques

Omar Abdul Razzaq
Department of Information Technology Engineering
Faculty of Technical and Engineering
University of Qom
Qom
Iran

Abstract

An elliptic curve cryptography (ECC)-based session-critical distributed authentication method is implemented in this study to enhance data security in wireless sensor Internet of Things (IoT) devices. ECC is chosen for its efficient key generation and compact key sizes, which are well-suited for resource-constrained IoT environments. The proposed approach aims to establish secure and reliable communication channels, ensuring robust authentication and protection against potential security threats. By leveraging ECC's cryptographic strengths, this work contributes to advancing the security infrastructure of IoT networks, addressing critical concerns related to data integrity and confidentiality. This study shows that the proposed WSN is capable of enhancing data transmission efficiency and reliability by exhibiting superior PDR and throughput performance.

Subject Classification: *11T71, 14G50.*

Keywords: *Network security, Sensor network, IOT.*

1. Introduction

Due to the vulnerability of these sensors, data security has become increasingly important. The nature of WSNs results in a large number of limited-resource sensors. WSNs can exploit an array of vulnerabilities. Consequently, attacks will become more complex and sophisticated as time goes on. Nowadays, hackers are capable of altering or modifying data while it is in transit and then sending it back to the users with the fabricated information. It is imperative to ensure that data confidentiality, integrity, authentication, and privacy are met. WSNs, therefore, must provide a secure environment for data transfers [1], [2]. Computational limitations, processing time constraints, energy

E-mail: diazrodr.od@gmail.com

consumption constraints, and efficiency constraints limit the capabilities of wireless sensor networks. In IoT deployments, most of the WSNs are periodically placed in unsupervised hazardous environments, capturing vital data [3], [4], [5]. A user's sensitive data cannot be compromised by users who have unauthorized access to it. A security vulnerability, attack, or threat in WSNs on IoT can also threaten the data security that is being transmitted. It makes users' lives difficult, as well as their data's security. Consequently, crucial data of users' needs to be protected with essential security measures. It is important to encrypt and authenticate the packets transmitted by wireless devices to ensure data integrity, confidentiality, and authenticity. Furthermore, due to their resource constraints and vulnerability to a variety of security vulnerabilities, it is common practice for WSNs to use lightweight encryption techniques in order to improve data security without degrading the performance of the network. It is necessary to use lightweight cryptographic protection as data volumes grow exponentially and are susceptible to alteration and destruction [6]. In addition to improving the efficiency and performance of sensor nodes, lightweight cryptography increases their energy consumption and security [3], [7]. As the name implies, sensor networks are systems that combine sensors and actuators with general-purpose computers. An environment monitoring system based on thousands or hundreds of low-cost, low-power wireless nodes will monitor and impact the environment [1]. There are a variety of limitations associated with sensor networks, including limited power supplies, limited bandwidth, very small memory sizes, and high energy consumption. Due to this, providing security becomes extremely challenging as shown in Figure 1.

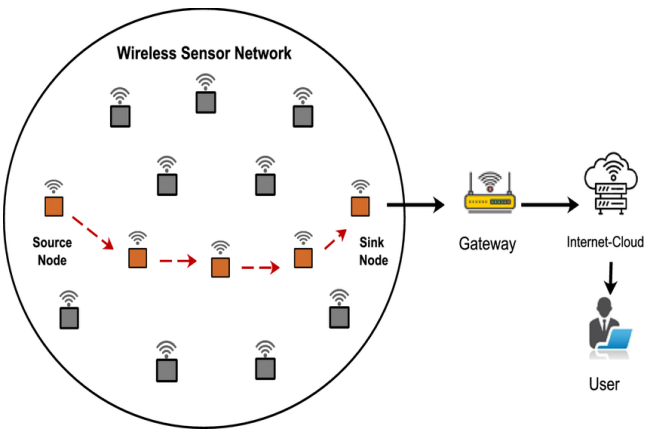

Figure 1
Wireless Sensor Network

2. Security Requirements In Wireless Sensor Network

As part of the security services provided in WSNs, information and resources are protected from attacks and misbehaviour. As part of WSN security, the following requirements must be met:

Confidentiality: The information must be kept confidential and hidden from unauthorized parties. Communication between nodes of many applications involves highly sensitive information. If a sensor network has neighbouring networks, there should be no leak of sensor readings. An encryption key that is known only to the intended recipients can be used to maintain confidentiality. Asymmetric key encryption is preferred in sensor networks with limited resources because public key cryptography is too expensive. A robust key distribution mechanism is essential for symmetric key approaches.

Authentication: When a message is authenticated, its origin is identified, thereby ensuring its reliability. The authentication in a WSN must satisfy the following requirements: [8], [9] Obtaining an authentication from the communicating nodes should be verified (ii) confirming the packets arrived from the sensor nodes should be verified. A secret key must be shared between the two parties to compute message authentication codes (MACs) for all conveyed data in instruction to achieve authentication. Utilizing the MAC key, the receiver verifies the genuineness of the message.

Integrity: Unauthorized parties must not alter data in order to maintain integrity. The authentication of data can also guarantee data integrity.

Availability: When a service or information is available, it ensures that the user can access it when they need it. Sensor networks are susceptible to many threats that could lead to loss of availability, including node capturing and denial-of-service attacks.

3. Related Work

An RFID authentication process has been developed using an approach RFID-ECC. In this research, the numerous vulnerabilities in IoT data security have been analyzed in order to improve it [10], [11]. A radio frequency identification scheme is developed using an ECC approach, which considers security weaknesses. With this process, the overall security requirements can be enhanced at a minimal cost. Using a content-centric network, the Author created an ECC framework for secure IoT communication [12]. The certificate-less public key infrastructure was designed to ensure security in resource-constrained IoT communications. In conjunction with the lightweight cryptosystem, elliptic curve cryptography is used to mitigate intermediate cryptographic attacks on data security.

The Author applied a combination of cryptographic algorithms to create a secure IoT-based healthcare data transmission model [13]. This process results in the creation of hybrid encryption schemes based on discrete wavelets combined with Rivest and the advanced encryption standard algorithm. IoT data transmitted via a hybrid encryption algorithm, including both text and images, is encrypted. Intermediary attackers find it difficult to identify the encryption algorithm combination. In hybrid encryption, patient confidentiality, capacity, and inaudibility can be maintained.

Data encryption schemes typically protect IoT parties. Much research has been conducted on encryption schemes [14], [15], [16], [17]. The authors of [18]

different network levels can be protected by ECC and Diffie-Hellman algorithms. In [14], an algorithm that protects privacy using homomorphic encryption with symmetric keys is proposed. The Author [19] describes a three-category key-management strategy for sensor nodes. The Author [20] sensors and BS are connected using a symmetric key. This method of transmission aims to achieve a high level of security, minimal energy consumption, and improved scalability. The paper presents a symmetric key cryptographic scheme for hierarchical clustered WSNs [15], [21]. Eavesdropping is the primary objective of the scheme. There is a known plaintext attack (KPA) in [16], which produces the same CS matrix every round. A symmetric key algorithm is fast and requires fewer operations every round [16]. A random mixing bijection is used to merge and blend some steps of the round function. The authors of [22-24] proposed encrypting and decrypting sensor data by Cellular Automata Rules (CA Rules). Data privacy and security were provided by all the algorithms above, but their high computational complexity prevents them from being used to secure IoT devices with limited power and storage.

4. Methodology

For managing data security in wireless sensor Internet of Things devices, elliptic curve cryptography (ECC) is applied in this study. As part of the ECC method, the key value is generated for the sender and receiver. A session's duration and interruptions are accounted for during authentication. For data security, a one-time password is used to authenticate each session. A secure IoT data management process is implemented to prevent insider attacks. Time stamps are used to generate session keys. Incompatibility between previous session keys and current session keys can provide resilience to both insider attacks and reply attacks. Further dictionary attacks can be exploited in wireless sensor IoT devices through end-to-end authentication with the ECC algorithm and linear hashing.

a. *Authenticating Sessions*

Smart applications are created by collecting data from wireless sensor IoT devices. Detailed information is transmitted between locations; data security and privacy should be maintained. Distributed environments with authentication are used to store and send information in order to ensure its safety. The verification procedure involves verifying a user's identity in order to access IoT resources, data, and applications. Accountability and trust are managed through authentication. One-time password schemes are used to transmit wireless sensor IoT device information, which is only able to reduce the possibility of insider attacks. The system enables secret communication between the sender and receiver by generating a list of passwords. Passwords are only selected from a list that is saved on the server by the sender. Depending on the user's selection of password, the password is changed, preventing insider attacks by revealing the password. It consists of two steps: registration (users of IoT devices registering

their data to the server) and login and authentication (the server authenticating the user).

b. *Registration*

Registration is the first step in session-critical distributed authentication. The server receives the secret key from every wireless sensor IoT device. SK stands for the secret key. Each session (GR) is generated by generating random numbers D based on the timestamp T. As a result, we denote the session key as

$$GR = D||T \tag{1}$$

Servers generate key values based on session keys and secret values and send them to users as $R = \mathrm{SK} \oplus GR$. The user receives a computation of R value, which is then used to estimate the session key GR value

$$GR = \mathrm{SK} \oplus R \tag{2}$$

A random value for E is generated by the user, and the initial SR value is generated as a result of this. Equation (3) is used to calculate the value.

$$SR = E + \mathrm{SK} \tag{3}$$

It is then necessary to determine the secret key E and session key SR, and the server should be informed about the number of times N. Perform the $SR \oplus GR$ and $N \oplus GR$ before transmitting $SR \oplus GR$ and $N \oplus GR$.

User-transmitted information, including $SR \oplus GR$ and $N \oplus GR$ were processed by the server to determine N and SR values. Following are the steps taken by the server to compute the password based on the SR of the initial key and the linear hash function:

$$P_0 = H^N(SR) \tag{4}$$

As defined by Equation (4), H represents the linear hash function, which means the dynamic structure of the data implements the hash table when generating passwords. Password generated by $P_0 = P_0 \oplus GR$. P_0 and N values are saved in the server database as generated passwords. Users are given session IDs by servers when they login to IoT devices. As a result of this process, it is possible to authenticate when accessing the IoT details in a distributed environment. Equation (5) is also used to compute P_0, P_1 and P_2.

$$P_1 = H^{N-1}(SR); P_2 = H^{N-2}(SR) \tag{5}$$

P_0, P_1 and P_2 are XORed with GK, the session key, and passed along to the user. A representation of the XOR process can be found in Equation (6).

$$\left.\begin{matrix} P_0 \oplus GR \\ P_1 \oplus GR \\ P_2 \oplus GR \end{matrix}\right\} \tag{6}$$

Equation (6) XORs the received values to get the original passwords P_0, P_1 and P_2 using the session key GR. It is through the registration process itself that end-to-end authentication is enhanced here. During every key transmission, the secret is enabled while the user and server communicate. In both wireless sensor IoT device data transmissions and communications, this secret communication

process is robust against insider attacks. Due to the presence of a third party, the authentication ensures an end to IoT communication when equal values are encountered. Upon completion of wireless sensor IoT device user registration and information transfer from a single location to another, data transfer can begin. It has been possible to access the data from the IoT devices by logging in and authenticating. The following are the steps involved in securing data access.

c. *Login and Authentication*

An authentication process is essential to validating a user's identity and giving them access to the system. As soon as the user logs into the server to access the data, a new session key is generated by the server called GR. GR is generated according to T timestamp and D random number. A hash function, H, and initial key SR, defined by Equation (7), are used by the server to estimate the password.

$$P_{t-1} = H^{C+1}(SR) \tag{7}$$

$N - t$ is used to compute C, and H is used to compute H. To perform authentication, the server uses the P_{t-1} value in conjunction with the session key, such as $P_{t-1} \oplus GR$ and $GR \oplus SEED$. Users then calculate the session key value by using the computed values from Eq. (8).

$$GR = P_{t-1} \oplus (p_{t-1} \oplus GR) \tag{8}$$

A comparison is made between the computed value and the user's timestamp. As a result of Equation (9), an estimate of SK can be made if the value is valid.

$$\text{SK} = GR \oplus (R) \tag{9}$$

In Eq. (9), $R = \text{SK} \oplus GR$. Verifying the identity of the user is done by checking the estimated SK value against the server memory. Authentication is successful if the computed value matches the database value.

Upon verifying the server's identity, the session key is $XORed\ (GR \oplus P_t)$ with the password. $P_t = GR \oplus (GR \oplus P_t)$ is used by the server to compute the password. P_{t-1} is calculated by taking the hash value of P_t and dividing by the estimated P_t Value. In the case of a match between P_t and P_{t-1}, the user is verified. N is updated with C on the server. Here, $C = N - t$ on the server. In preparation for the next logins and data access, the server has generated the next password and sent it to the user. In this example, Eq. (10 is used to generate the password.

$$P_{t+1} = GR \oplus (GR \oplus P_{t+1}) \tag{10}$$

P_{t+1} values are stored in the database so that subsequent logins and IoT wireless sensor data access are secured. As sessions are maintained at every timestamp, insider attacks cannot occur because passwords are updated every time. Secret keys and session keys enabled secure data access in this study. As a final step, the Elliptic Curve Cryptography (ECC) method is used to encrypt user information after the details have been verified with the server database.

d. *Elliptic Curve Cryptography-Based Authentication*

A public-key cryptographic system encrypts information and keeps it confidential. As a result of the ECC approach, IoT data can be accessed securely and privately. A one-time critical session-based authentication process ensures user and server authentication. A third-party server's data is accessed using end-to-end authentication during the user verification process.

With this method, concealed authentication is performed using an enhanced elliptic curve cryptography algorithm (ECC). As a result of the elliptic curve equation, the public and private keys are generated without involving traditional prime numbers. Third parties will find it difficult to guess the elliptic curve-based generated keys due to their robustness and complexity. This algorithm is designed to consume the least amount of computing resources and to ensure the highest level of data security possible. Based on Eq (11), we can form the Equation for an elliptic curve $G(p)$.

$$Y^2 = X^3 + cx + d \tag{11}$$

Y^2 is represented by the elliptic curve in Eq. (11); c and d are real numbers.

Parameters are required to create a public key and a private key. Public keys are defined by an elliptic curve, and secret keys are randomly chosen by the user among $[2, n-2]$. The user and server exchange key values based on the ECC algorithm for authentication purposes. ECC-related key values have the greatest impact on overall system security. Security is enhanced by registering, logging in, and authenticating wireless sensor IoT devices.

A successful authentication between the user and server allows access to information on the wireless sensor IoT device. ECC is used to generate the initial key, which is more secure and difficult for intermediates to guess. Registration, logging in, and authentication are all dependent on the secret key and session key to maintain data security. Additionally, the generated session keys with passwords are varied, making it difficult for the authenticated person to guess from session to session. Users select the passwords themselves, which are different every time. The created system, therefore, effectively addresses the insider attack issue.

5. Result and Analysis

Comparisons are made between the proposed Identity-Based Encryption (IIBE) and Identity-Based Authenticated Encryption (IBAS) models when measured by packet delivery ratio (PDR), throughput, delay, and encryption time. A node's performance value is indicated on the Y-axis, while its number is indicated on the X-axis. This Figure 2 compares the proposed model to the current IIBE and IBAS models in terms of packet delivery ratio (PDR) performance measurements for IoT-based Wireless Sensor Networks. Nodes are represented by the X-axis and PDR values by the Y-axis. The results indicate that the proposed model significantly outperforms the IIBE and IBAS models. At 250 nodes, the proposed model achieves a PDR of 99%, whereas the IIBE and IBAS models attain PDR values of 92% and 93%, respectively. This higher

PDR indicates that the proposed model is more efficient in ensuring that data packets are successfully delivered across the network. The improved PDR can be attributed to the model's optimized routing algorithms and enhanced data handling capabilities. By achieving a higher PDR, the proposed model demonstrates greater reliability and effectiveness in maintaining robust communication within IoT-based WSNs.

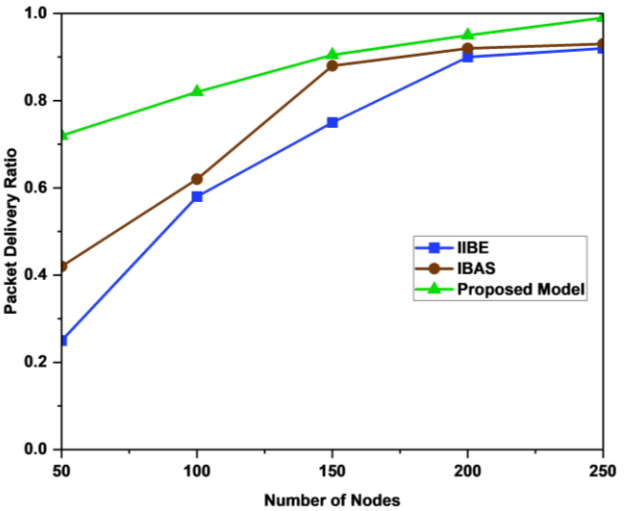

Figure 2
Packet Delivery Ratio versus number of nodes.

Based on the metrics of throughput performance, Figure 3 compares the proposed model with the existing IIBE and IBAS models. The X-axis represents different performance indicators, while the Y-axis depicts throughput values measured in (Kbps). According to the results, this model achieves a 360 Kbps throughput. In contrast, the IIBE model demonstrates a throughput of 340 Kbps, and the IBAS model achieves a throughput of 350 Kbps. This comparison underscores the superior data transmission efficiency of the proposed model compared to the current IIBE and IBAS models. The higher throughput of the proposed model signifies its capability to handle and process data at a faster rate, thereby improving overall network performance. This advantage can be attributed to optimized encryption algorithms and efficient data packet management techniques employed in the proposed model. In summary, Figure 3 emphasizes the enhanced throughput performance of the proposed model, highlighting its potential to enhance data transmission speeds and network efficiency compared to existing encryption models like IIBE and IBAS.

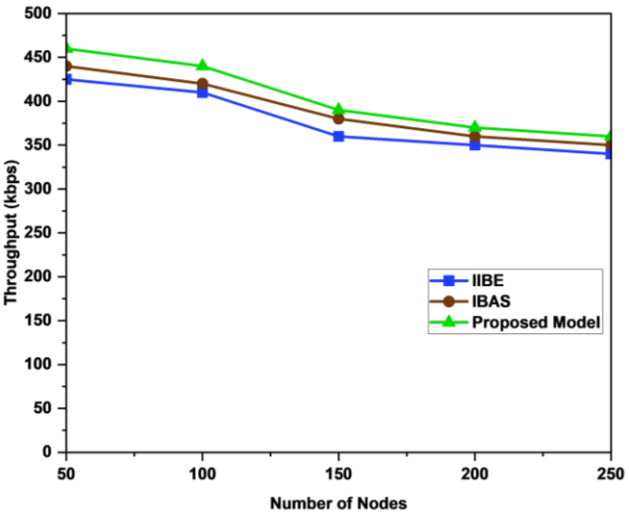

Figure 3
Average throughput (kbps) versus number of nodes.

In Figure 4, the proposed model is compared to the existing IIBE and IBAS models in terms of complete delay efficiency metrics. On the X-axis, node numbers are represented, while on the Y-axis, they are measured as end-to-end latencies. The findings demonstrate a significant improvement in delay efficiency with the proposed model. Specifically, the proposed model achieves an end-to-end delay of 49 seconds, which is considerably lower than the delays observed with the IIBE and IBAS models. The IIBE model records an end-to-end delay of 84 seconds, while the IBAS model shows a delay of 63 seconds.

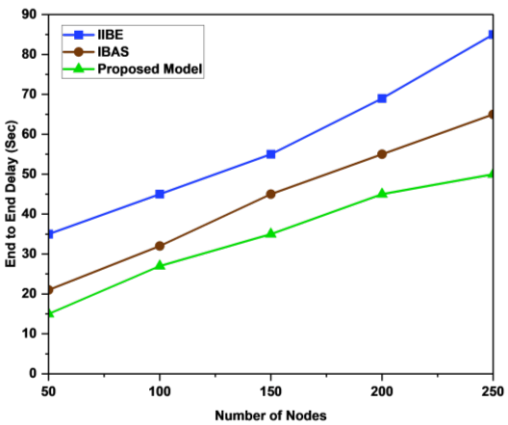

Figure 4
End to end delay (sec) versus number of nodes.

End-to-end latency was reduced by the proposed model, demonstrating its efficiency. The optimized processing algorithms and efficient handling of data packets contribute to this improved performance. This model enables the system to process data quickly and respond in real-time by minimizing delays, thus making it more suitable for real-time applications. Overall, Figure 4 underscores the proposed model's superior delay efficiency compared to existing models, demonstrating its potential to improve network performance and reduce latency in various applications significantly.

Figure 5 provides a detailed comparison of the proposed model's encryption time performance against the current Identity-Based Encryption (IIBE) and Identity-Based Authenticated Encryption (IBAS) models. As the X-axis represents plaintext size, the Y-axis shows the length of time that it took to encrypt the message. The comparison reveals that the proposed model significantly outperforms both IIBE and IBAS models in terms of encryption speed. For a plaintext size of 100MB, the proposed model completes the encryption process in just 70 seconds. In contrast, the IIBE model takes 185 seconds, and the IBAS model requires 90 seconds to encrypt the same amount of data. This performance improvement can be attributed to the optimized algorithms and efficient processing techniques employed in the proposed model. The reduction in encryption time demonstrates the model's efficiency, making it a more practical and effective solution for scenarios where rapid data encryption is crucial. A real-time data processing and secure communication application may benefit the most from this advantage.

Overall, Figure 5 highlights the proposed model's superiority in encryption speed, underscoring its potential to replace existing encryption methods with a faster and more efficient alternative. This improvement can enhance the performance of systems relying on encryption for data security, providing quicker encryption without compromising security standards.

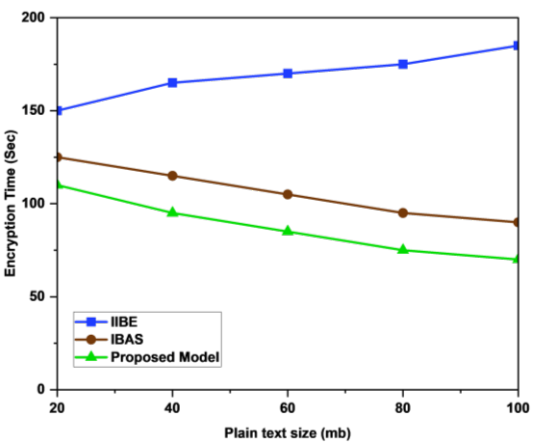

Figure 5
Encryption time (sec) versus number of nodes.

6. Conclusion

This study has demonstrated the efficacy of employing elliptic curve cryptography (ECC) in session-critical distributed authentication for enhancing data security in wireless sensor IoT devices. By leveraging ECC's efficient key generation and compact key sizes, we have addressed the challenges posed by resource constraints in IoT environments while ensuring robust cryptographic security. The implementation of ECC-based authentication has shown promising results in establishing secure communication channels and mitigating potential security vulnerabilities. The proposed model demonstrates superior performance across multiple metrics. It achieves a significantly reduced encryption time and end-to-end delay compared to IIBE and IBAS, enhancing data transmission efficiency. Moreover, the proposed model exhibits a higher Packet Delivery Ratio (PDR), ensuring reliable data delivery in WSN environments. Notably, the proposed model also achieves a higher throughput, indicating improved data handling capabilities. The results highlight the proposed model's potential to advance data security and network efficiency in modern IoT applications. Further research could explore optimizations and enhancements specific to IoT deployments, such as lightweight ECC variants or integration with emerging authentication protocols. These efforts will be crucial in advancing the reliability and scalability of IoT security solutions, ultimately fostering trust and resilience in connected IoT ecosystems.

References

[1] Mohd Azlishah Burhanuddin, Ahmed A.-J. Mohammed, Rozeha Ismail, Murtadha E. Hameed, Ahmed N. Kareem, and Hairulnizam Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *Journal of Telecommunication, Electronic and Computer Engineering* (JTEC), vol. 10, no. 1–7, pp. 17–21 (2018).

[2] Nitesh Kumar, Priyanka Rani, Vijay Kumar, Pradeep Kumar Verma, and Deepak Koundal, "Teeech: Three-tier extended energy efficient clustering hierarchy protocol for heterogeneous wireless sensor network," *Expert Systems with Applications,* vol. 216, pp. 119448 (2023).

[3] D. Aakash and P. Shanthi, "Lightweight security algorithm for wireless node connected with IoT," *Indian Journal of Science and Technology,* vol. 9, pp. 1–8 (2016).

[4] Surjeet Singh, Pradeep Kumar Sharma, Sang-Yong Moon, and Jong Hyuk Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient*

Intelligence and Humanized Computing, vol. 15, no. 2, pp. 1625–1642 (Feb. 2024), doi: 10.1007/s12652-017-0494-4.

[5] Nitesh Kumar, Priyanka Rani, Vijay Kumar, Sachin V. Athawale, and Deepak Koundal, "THWSN: Enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks," *IEEE Sensors Journal*, vol. 22, no. 20, pp. 20053–20062 (2022).

[6] Pankaj Tiwari, Virendra P. Saxena, Rakesh G. Mishra, and Dharmendra Bhavsar, "Wireless sensor networks: Introduction, advantages, applications and research challenges," *HCTL Open International Journal of Technology Innovations and Research* (IJTIR), vol. 14, pp. 1–11 (2015).

[7] Nazia Hussain, Priyanka Rani, Hemant Chouhan, and Umesh Singh Gaur, "Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues," in *Federated Learning for Internet of Things Applications*, pp. 169–183 (2022).

[8] Matt Welsh, "Resuscitation monitoring with a wireless sensor network," *Journal of the American Heart Association* (2003). [Online]. Available: https://cir.nii.ac.jp/crid/1571135650147360256. Accessed: Jul. 08, 2024.

[9] Ankit Singh, Nitika Sharma, Pardeep Kumar, Rajeev Kumar, Ashok Kumar, and Neeraj Kumar, "Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication," *IEEE Transactions on Consumer Electronics* (2024).

[10] Sourav Adhikari and Sudip Ray, "A Lightweight and Secure IoT Communication Framework in Content-Centric Network Using Elliptic Curve Cryptography," in Recent Trends in Communication, Computing, and Electronics, Amit Kumar Khare, U. S. Tiwary, Iqbal Kaur Sethi, and Naveen Singh, Eds., Lecture Notes in Electrical Engineering, vol. 524. Singapore: Springer Singapore, pp. 207–216 (2019). doi: 10.1007/978-981-13-2685-1_21.

[11] Priyanka Rani, Pradeep Narayan Singh, Surbhi Verma, Naimat Ali, Pradeep Kumar Shukla, and Mowafa Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–14 (2022).

[12] Mohamed Elhoseny, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Sameh A. Shawkat, Nallagatla Arunkumar, and Ahmed Farouk,

"Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608 (2018).

[13] Ming Wang, Zhi Zhou, and Chunmei Ding, "Blockchain-Based Decentralized Reputation Management System for Internet of Everything in 6G-Enabled Cybertwin Architecture," *Journal of New Media*, vol. 3, no. 4 (2021). [Online]. Available: https://cdn.techscience.cn/uploads/attached/file/20211105/20211105083622_39693.pdf. Accessed: Jul. 08, 2024.

[14] Soumaya Ben Othman, Ahmed A. Bahattab, Anis Trad, and Hatem Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889 (Jan. 2015), doi: 10.1007/s11277-014-2061-z.

[15] R. Geetha and E. Kannan, "A hybrid key management approach for secure communication in wireless sensor networks," *Indian Journal of Science and Technology*, vol. 8, no. 5, pp. 1–8 (2015).

[16] Djamel Eddine Boubiche, Samira Boubiche, and Abdelhamid Bilami, "A cross-layer watermarking-based mechanism for data aggregation integrity in heterogeneous WSNs," *IEEE Communications Letters*, vol. 19, no. 5, pp. 823–826 (2015).

[17] Bhupesh Bhola, Mukesh Prasad, Ashutosh Sharma, Nilesh Dhanjani, and Shivam Bansal, "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," *IET Communications* (2022).

[18] Wissam Abdallah, Noureddine Boudriga, Do-Hyeun Kim, and Seungmin An, "An efficient and scalable key management mechanism for wireless sensor networks," in 2015 17th International Conference on Advanced Communication Technology (ICACT), *IEEE*, pp. 480–493 (2015). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7224913/. Accessed: Jul. 08, 2024.

[19] N. Suganthi and S. Vembu, "Energy efficient key management scheme for wireless sensor networks," *International Journal of Computers Communications & Control*, vol. 9, no. 1, pp. 71–78 (2014).

[20] Brahim Kadri, Mohammed Feham, and Amar Mhammed, "Efficient and Secured Ant Routing Algorithm for Wireless Sensor Networks," *International Journal of Network Security*, vol. 16, no. 2, pp. 149–156 (2014).

[21] Priyanka Rani and Rakesh Sharma, "IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), *IEEE*, pp. 1–6 (2023).

[22] Sajal Roy, Joydeep Karjee, Upendra Singh Rawat, and Nilanjan Dey, "Symmetric key encryption technique: a cellular automata based approach in wireless sensor networks," *Procedia Computer Science*, vol. 78, pp. 408–414 (2016).

[23] Azmi Shawkat Abdulbaqi, Israa Falih Muslim, Asraa A. Abd Al-Ameer, and Ahmed J. Obaid, "Healthcare surveillance based on cloud computing utilizing mobile devices," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1–8, DOI: 10.47974/JDMSC-1566.

[24] Niran A. Abdulhussein and Ahmed J. Obaid, "A landscape view of news recommendation systems based on MIND dataset," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1–12, DOI: 10.47974/JDMSC-1617.

Received December, 2024