A Three-phase hybrid cryptography algorithm: Utilized in public sensor network for data security with an enhancement of hashing algorithm

[1]Dhirendra Kumar Shukla, [2]*Osamah Khalaf, [3]Rohith Vallabhaneni, [4]Santosh Kumar Srivastava, [5]Sameer Algburi

Abstract: Cryptography, which is the practice of securing information by converting it into a form that is unintelligible to unauthorized individuals, is widely recognized as one of the most effective technologies for enhancing the security of Wireless Sensor Networks (WSNs). In this particular research endeavor, the authors introduce and elucidate upon the Three Phase Hybrid Cryptographic (TPHC) algorithm, a novel approach that combines both symmetric and asymmetric cryptographic algorithms to achieve the desired security objectives. By incorporating well-established encryption techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and a modified version of the Rivest-Shamir-Adleman (RSA) algorithm, TPHC is able to provide both confidentiality and authentication for the transmitted data within the WSN. Moreover, to ensure the integrity of the information, TPHC is complemented with a distinctive hashing algorithm that is specifically designed for this purpose. This proposed hash function exhibits adherence to the fundamental properties of conventional hashing, namely, one-wayness, second pre-image resistance, collision resistance, and the avalanche effect. The empirical results of this investigation unequivocally establish the dominance of the TPHC technique in comparison to the current WSN algorithm across multiple performance measures, such as computation time, size of encrypted data, size of digested data, and energy utilization.

Keywords: AES, DES, modified-RSA, hybrid cryptographic algorithm, hashing, digest

1. Introduction

Wireless sensor networks (WSNs), which have a variety of military and nonmilitary uses, are made up of a collection of tiny nodes that gather data from a specific area. WSNs lack a specific infrastructure or architecture, and their constituent nodes suffer significant energy, memory, and computing power constraints. Due to the limits of WSNs, we are unable to use standard procedures in these networks. The majority of cryptographic systems, for example, are based on asymmetric cryptography. However, because to their high energy consumption, these methods cannot be employed in WSNs. As a result, methods should be offered in WSNs that address the specific characteristics and limits of these networks. Homogeneous and heterogeneous networks are two types of WSNs. All nodes in homogeneous networks have the same characteristics in terms of energy utility, memory management, and computing power. Furthermore, they all perform the same job in networks. Some studies [1, 2] have pointed out that these networks have their own limits. Because data connection between sensors is crucial, especially in military applications, and data is transferred by the help of wireless media, a healthy, security mechanism for data integrity and secrecy should be present. One of the major difficulties are, how to generate a key management protocols with reference to similarities/ symmetric cryptography is launching shared secret keys among nodes so that they may encrypt

data and also use elementary security services such as message secrecy, data veracity, and authentication using these generated keys.

Routing security, secure location, and key management and cryptography are some of the solutions that exist to address these challenges [Fouchal et al., 2014; Hayajneh et al., 2013; Lasla et al., 2014; Farouk et al., 2014]. The finest instrument for dealing with security issues is cryptography, which is one of these. The importance of cryptography in the transit of data is critical [Maliberan, 2019]. The art of hidden writing is called cryptography. Real information is disguised or buried in another message and sent across the network in this case. Figure 1 depicts the entire cryptographic procedure [Hasan et. al., 2021]. Message integrity is ensured through hashing, which is employed after cryptography. A digest is the result of a hash function, which transforms an arbitrary length of input into a defined size. Figure 2 depicts the fundamentals of hashing (Yaksic, 2003).

Many scientists are working on it, and we've compiled a list of some of the works that might help you think more deeply about this task. Hasan et al. 2021 gave a comprehensive study of cryptographic methods grounded on timing complexity, cypher text size, and also the encryption, decryption performance. They used maximum key size to simulate a guessing attack on certain cryptographic systems. They ran algorithms five times for the identical plaintext and compared the results. They employed text having password-sized and paragraph-sized text for simulation purposes, that resulted in a reasonable execution. For S2aaS architecture, Bentahar et al., 2021 suggested a key agreement technique that was efficient and secure for users to surf safely. The authors employed a fuzzy logic extractor and ECDH techniques in concurrence with symmetric cryptographic methods, and hash functions to achieve a significant key agreement. Cloud was regarded as an unstable node in their simulation of the S2aaS architecture [22-35].

Khari et al., 2019 created the elliptic Galois cryptography protocol to encrypt data from various medical sources, then utilised matrix XOR to turn the encrypted data into a low complexity picture. The authors utilised an optimization method to choose the image's cover block. Data was retrieved from the picture and decrypted after the findings were analysed and compared to current approaches. The authors of Dobraunig et al., 2021 gave specifications for two Ascon versions, 128 and 128a, which offered encryption for high-end devices. For a lightweight encryption mechanism, this method was picked as the initial option. They renamed Ascon-hash and Ascon-Xof after introducing hashing into the conventional Ascon approach. They compared the suggested model's results to current cryptanalysis. The pioneer system known as HIBE was built by Langrehr et al., 2020. The approach for identifying secret users with variable lengths was at the heart of the strategy, and it was based on the Matrix Diffie-Hellman assumption. They constructed two cypher texts, one with a fixed size and the other with a linear size. With the aid of Naor transformation, they were able to create a secure identity-based signature [36-45].

Devi et al., 2021 combined symmetric and asymmetric algorithms to create hybrid algorithms that provide robust security and key management. They implemented their method using JAVA programming, and after compiling the results, it was determined that the suggested hybrid algorithm gave better security than any other approach. They tested RC5, AES, and RC6, using encryption and decryption time with varied text sizes and memory needs as comparative factors. Apart from that, it complied with all security requirements and was impervious to wormhole, quantum, spoofing, blackhole, and DoS attacks. Rizk et al. (2015)

created a hybrid method that combines ECC, AES, XOR-DUAL-RSA, and MD5. They put their work on NS2 and found that their method was better in terms of cypher text size and energy usage after analysing the data. Not only that, but they've demonstrated that their picture encryption technique is resistant to a variety of assaults [46-55].

Subasree et al. (2010) presented a method based on ECC, Dual-RSA, and MD5. They used VC++ to implement their algorithm. They compared RSA with DUAL-RSA and found DUAL-RSA to be superior to RSA. They built their method for people, such as sender, recipient, and invader, and shown that it outperforms other algorithms in terms of performance. Kumar et al. (2012) devised a hybrid approach that combines AES and ECC. They also employed MD5 to hash the cypher text, and their technique was conducted in a sequential way, which resulted in a longer execution time. Ren et al. (2010) improved Bluetooth communication security by creating a hybrid approach that included DES (for data transfer) and RSA (for authentication) (for encryption). Their method was simpler and more efficient, and also improved the degree of security and secrecy. Ramaraj et al. (2009) presented a technique that used key servers to tackle key management difficulties. AES-Rijndael, RSA, and SHA-512 methods were utilised in their suggested protocol. Session Key Establishment Phase, Secure Transmission Phase, and Secure Decryption Phase are the three phases of their algorithm. Their hybrid encryption approach improved the efficiency of cryptographic algorithms, and they found that their protocol provided secrecy, integrity, and authenticity using the AES-Rijndael algorithm and the hash function. Bhole et.al. 2016 introduced a hybrid technique by combining both symmetric and asymmetric cryptographic algorithms, that is, AES and ECC, XOR-Dual RSA and MD5. They used JAVA platform with Netbeans IDE for the implementation. They have divided their plain text into two parts and applied AES and ECC on first part of plain text and XOR-DUAL-RSA on second part [56-65].

In 2021, Fahmi et al. used the AES and HMAC algorithms to create a Hybrid Cryptography security mechanism. They used a Brute-Force attack and a man-in-the-middle assault to test the confidentiality and integrity criteria, respectively. Their research was carried out on a sensor node that included an LED, an ultrasonic sensor, and an ESP32. Their mechanism's main feature was detecting the attacker's data changes and controlling the brute force assault. Their encryption procedure took 409 microseconds, while their decryption process took 7304 microseconds on average. Hamid et al. introduced a symmetric cryptography-based solution for key formation in hierarchical wireless sensor networks. Symmetric cryptosystems are a suitable choice for sensor networks since they require less energy. Although symmetric cryptosystems need a lot of memory, this disadvantage may be mitigated with the right strategies.

This research paper is structured in the following way. In part 2, the literature review was covered, followed by a discussion of the problem definition. The suggested work has been explained in section 4, and the findings and analysis have been completed in part 5. Section 6 ends with a conclusion and recommendations for the future.

2. Problem definition And Proposed Work

The existing cryptography methods take longer to execute and produce a huge digest. As a result, a unique cryptographic technique is required to minimise time consumption and increase the energy efficiency of the nodes.

2.1. Cryptography and Hashing Model

The three Phase Hybrid Cryptography model has been updated to include the proposed Hashing Technique. Figure 3 shows plain text that has been separated into three pieces and then AES, DES, and modified RSA have been applied to all three portions at the same time. The recipient has received these three encrypted messages, which have been concatenated. The Proposed Hash function was applied to each encryption text (C1, C2, and C3), and the hash values (H1, H2, and H3 accordingly) were provided to the recipient. For authentication, cryptography was utilised, and the hashing technique was used for integrity. Figure 4 shows the encrypted text and hash values received by the recipient. The receiver deciphers the encrypted text and hashes each of the three pieces. If the three portions' computed hash values (h1, h2, and h3) match the received hash values (H1, H2, and H3), the message will be accepted; otherwise, it will be rejected. After receiving the communication, the plain text was obtained using the recommended decryption techniques.

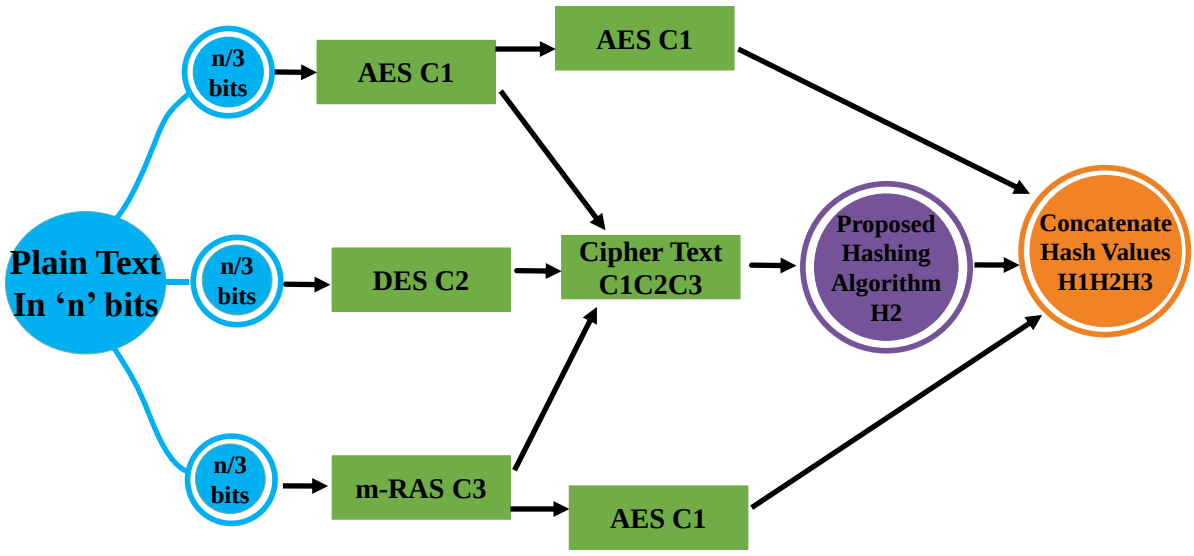

Fig.1 Detail on Proposed Encryption Phase Model

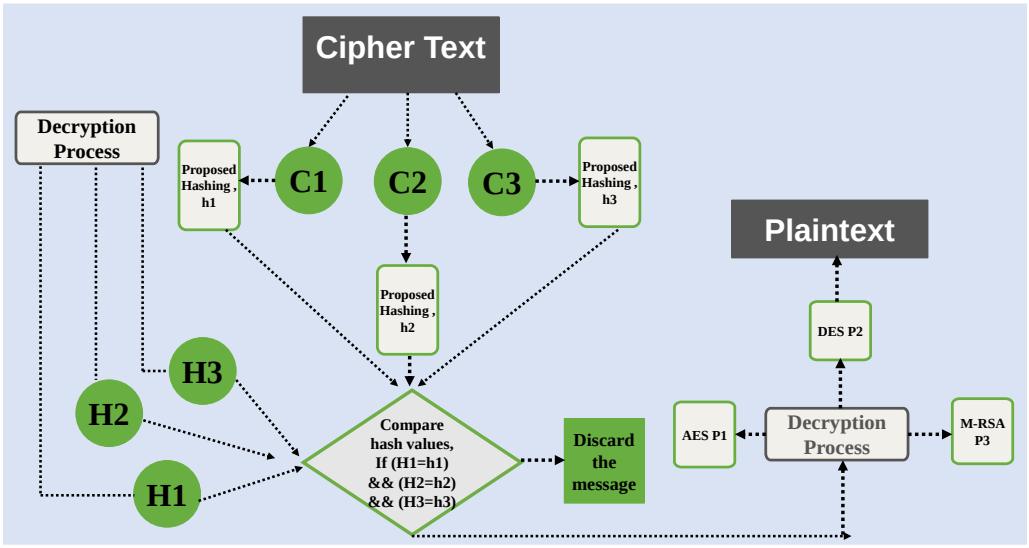

Figure 2: Proposed Decryption Phase Model by the author.

2.2.TPHC algorithm

The techniques for encryption and decryption are detailed in the paper Pooja, Chauhan R. K., 2020. To begin, the input text is separated into three pieces, and then AES, DES, and modified RSA are applied to all three portions at the same time, using three distinct phases.

Encryption, Decryption, Hashing Phase Algorithm:

PHASE I: $m_i = \sum_{i=0}^{\frac{n}{3}-1}(Bi)$ $\quad 0 \le i \le n/3\text{-}1$

$c_i = AES_{enc}(m_i, k_i)$; $\quad C1 = c_i$

PHASE II: $m_i = \sum_{i=n/3}^{\frac{2n}{3}-1}(Bi)$ $\quad n/3 \le i \le 2n/3\text{-}1$

$c_i = DES_{enc}(m_i, k_i)$; $\quad C2 = c_i$

PHASE III: $m_i = \sum_{i=2n/3}^{n-1}(Bi)$ $\quad 2n/3 \le i \le n\text{-}1$

$c_i = m\text{-}RSA_{enc}(m_i, k_i)$; $C3 = c_i$

Combine all the cipher texts and send to the receiver;

$C = C1C2C3$

Figure 3: Step by step process of encryption algorithm

PHASE I: $C_i = \sum_{i=0}^{\frac{n}{3}-1}(Bi)$ $\quad 0 \le i \le n/3\text{-}1$

$m_i = AES_{dec}(C_i, k_i)$; $P1 = m_i$

PHASE II: $C_i = \sum_{i=n/3}^{\frac{2n}{3}-1}(Bi)$ $\quad n/3 \le i \le 2n/3\text{-}1$

$m_i = DES_{dec}(C_i, k_i)$; $P2 = m_i$

PHASE III: $C_i = \sum_{i=2n/3}^{n-1}(Bi)$ $\quad 0 \le i \le n/2\text{-}1$

$m_i = m\text{-}RSA_{dec}(C_i, k_i)$; $P3 = m_i$

On Combining the plain texts we will get original message.

$P = P1P2P3$

Figure 4: Step by step process of Decryption Algorithm

The receiver divides the encrypted text into three pieces and uses decryption techniques such as AES, DES, and modified RSA to decode it.

Input: Message of arbitrary length.

Output: Digest of fixed size, i.e., 128 bits.

Begin

1. Apply padding of 10^* bits.
2. Append length of message (binary form) to the previous step output, so that length of final message is in the multiples of 512.
3. i=0, j=-1
4. while (i<n) {
5. j=j+1
6. Bj=M(i,i+511)
7. i=i+512}
8. i=0
9. while (i ≤ j) {
10. Bi1=Bi (0,127)
11. Bi2=Bi (128,255)
12. Bi3=Bi (256, 383)
13. Bi4=Bi (384,511)
14. i= i+1}
15. i=-1
16. while (i <j) {
17. i=i+1
18. Bi=Bi1 XOR Bi2 XOR Bi3 XOR Bi4}
19. digest=B0 XOR B1 XOR B2 XOR ..... Bj

End

Figure 5: Step by step process of generating Hashing Function [10]

3. Simulation and Analysis

The algorithm was simulated in Matlab 2017b, and the suggested work was compared to that of Subasree, Kumar, Ren, Ramaraj, and Bhole. There are several fixed parameters in MATLAB, which are types of nodes (20), the number/ types of rounds (10), and the size of plain text (192 bytes). Three separate graphs, namely the number/ types of packets transmitted to the Base Station, the dead nodes, and the total of surviving nodes' energy, are displayed in one parent graph in the following graphs. Subasree's work is shown in figure 8, Kumar's work is shown in figure 9, Ren's work is shown in figure 10, Ramaraj's work is shown in figure 11, Bhole's work is shown in figure 12, and planned TPHC is shown in figure 13.

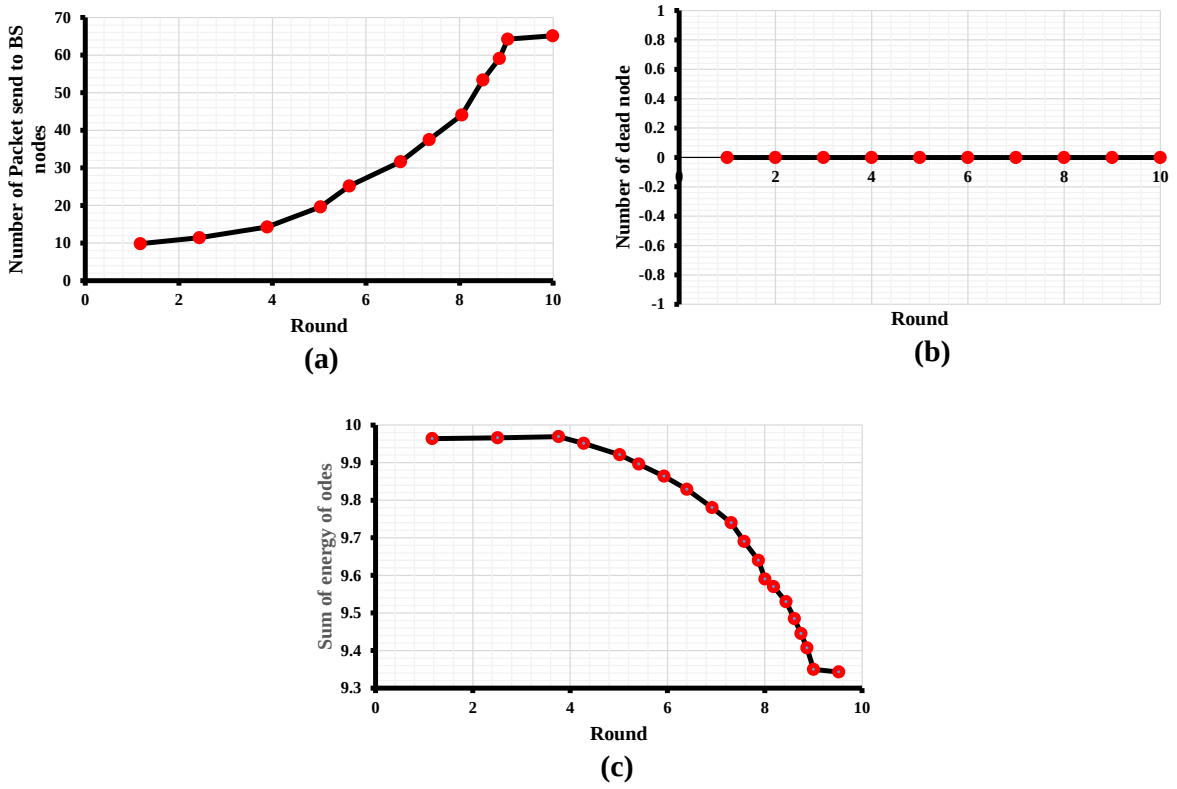

Figure 6: Subasree Work define and calculate various parameters such as (a) Round vs. Number of packets send to BS, (b) Round vs. number of dependent node, (c) Round vs. Sum of energy of nodes.

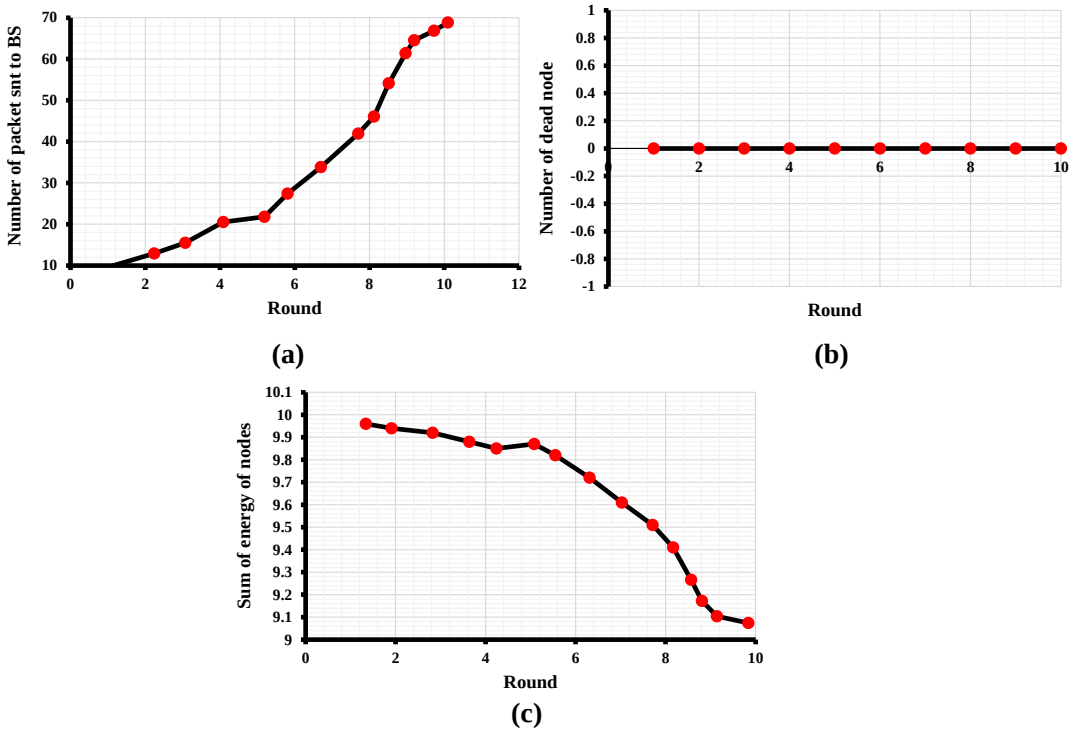

Figure 7: Ren Work define and calculate various parameters such as (a) Round vs. Number of packets send to BS, (b) Round vs. number of dependent node, (c) Round vs. Sum of energy of nodes.

Figure 2: Ren work

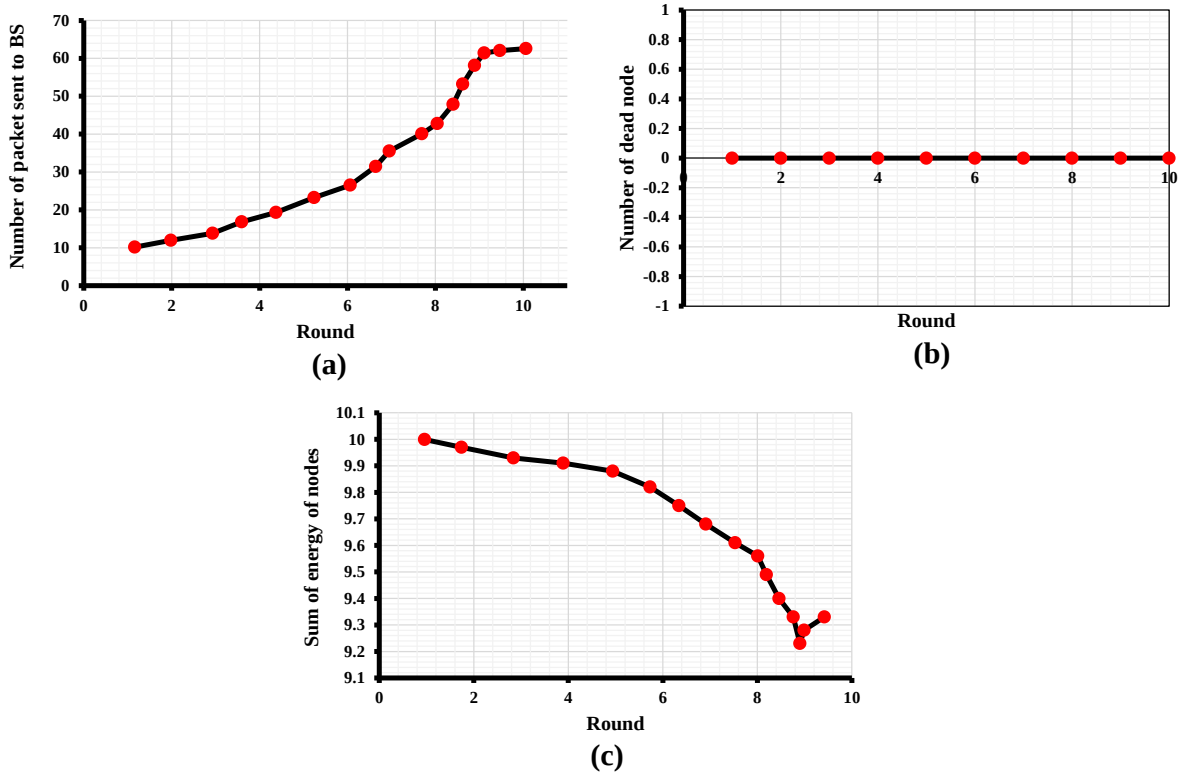

Figure 8: Ramaraj Work define and calculate various parameters such as (a) Round vs. Number of packets send to BS, (b) Round vs. number of dependent node, (c) Round vs. Sum of energy of nodes.

It has been discovered that TPHC consumes the least amount of energy; as stated in Table 1, the sum of remaining nodes' energy is the greatest in TPHC. The major purpose of TPHC is to minimise energy usage. Other methods, however, are superior in terms of the amount of packets sent.

Table 1: Comparison with existing algorithms

Comparison Metrics	Subasree's Work	Kumar's work	Ren's Work	Ramaraj's work	Bhole's work	Proposed work
Number of Packets sent	65	60	68	62	69	62
Number of Dead nodes	0	0	0	0	0	0
Sum of nodes' energy after transmission	9.35	8.95	9.12	9.35	9.08	9.42

The TPHC algorithm is then compared against current hybrid cryptography algorithms with varied text sizes, such as 193, 609, 769, 1217, and 1537. Table 2 shows the execution time with respect to existing and suggested approach/ models. t

Table 2: Total execution time with respect to existing and suggested approach/ models.

Text size	Subasree's Work	Kumar's work	Ren's Work	Ramaraj's work	Bhole's work	Proposed Work
193	1.43044	3.3303	0.3163	2.1809	3.3362	0.5741
609	1.4423	2.4854	0.7645	1.6505	2.5021	1.9371
769	1.4474	2.4854	0.9949	1.8829	2.506	2.0983
1217	1.4599	5.1824	1.635	4.9382	5.2171	3.28217
1537	1.4667	5.6356	1.8447	5.6561	5.6771	4.2064

Figure 14 depicts the execution time of existing and suggested approaches with changing text sizes. The text size for five distinct files, 192, 608, 768, 1216, and 1536, is presented on the x-axis, while the execution time in seconds is shown on the y-axis.

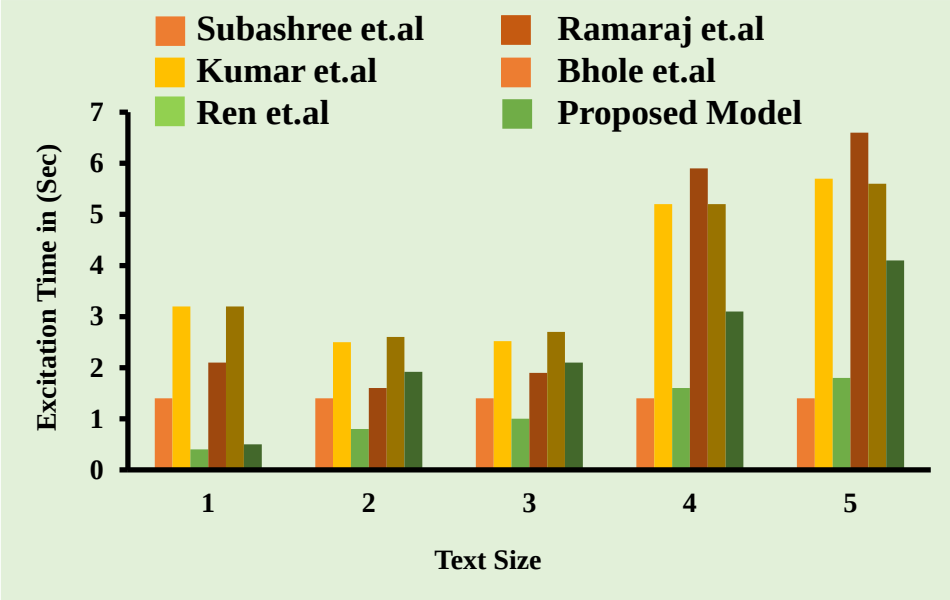

Figure 9: Total Execution time of existing and proposed

3.1.Overall Performance Index

The aforementioned algorithms' total performance has been calculated. Table 3 illustrates the normalized values of all four characteristics that are utilized as comparison metrics: number of packets transmitted to base station, number of dead nodes, sum of energy, and average execution time.

Table 3: Overall Performance Index

Parameters	Subasree et.al.	Kumar et.al.	Ren et.al.	Ramaraj et.al.	Bhole et.al.	Proposed work	Weight
Number of Packets sent to Base station	0.9420	0.8695	0.9855	0.8985	1	0.89855	0.3
Number of Dead Nodes	0	0	0	0	0	0	0.1
Sum of Energy	0.9925	0.9501	0.9681	0.9925	0.9639	1	0.4
Avg. Exe. Time	0.5712	0.0017	0.9051	0.3462	0	0.8279	0.2
Overall Performance Index	**0.7938**	**0.6412**	**0.8639**	**0.7358**	**0.6855**	**0.8351**	

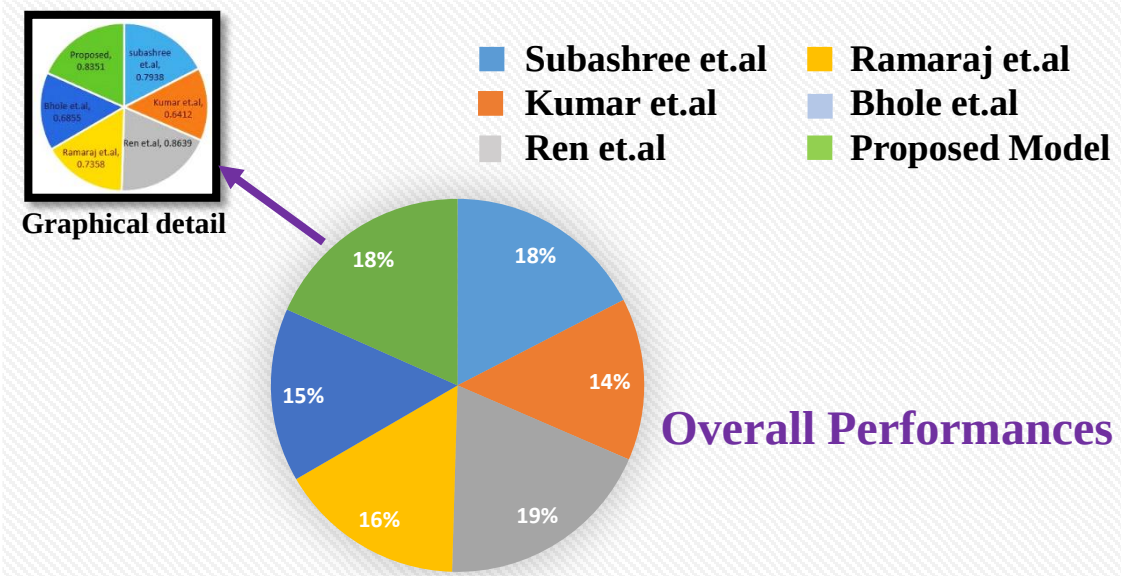

Figure 10: Overall Performance Index for various model

The total performance graph of the six methods is shown in Figure 15. The figure 15 was used to examine it. Ren's work is superior to the others. When compared to subasree's, kumar's, ramaraj's, and bhole's algorithms, the TPHC method trails behind Ren's approach by 0.0288 factor, which is a very minor amount.

4. Conclusion and Future Scope

The three Phase Hybrid Cryptographic (TPHC) algorithm, which combines three existing techniques and runs in parallel, has been presented. In terms of the number of packets delivered, the number of dead nodes, the total of energy remaining, and execution time, TPHC was compared to an existing method. Following the investigation, it was discovered that TPHC is the better method in terms of energy conservation, while the remaining parameters are average. This technology can be further developed such that it can be used to detect and eliminate attacks like clone attacks. The proposed hash function was created in a straightforward manner and compared to existing hash functions. It may be used to see if the suggested solution is resistant to current assaults like as brute-force attacks, birthday attacks, and so on.

References

1. Farouk, F., Rizk, R., Zaki, F.W., 2014. Multi-level stable and energy efficient clustering protocol in heterogeneous wireless sensor network. IETWirel. Sens. Syst. 4 (4), 159–169, http://dx.doi.org/10.1049/iet-wss.2014.0051.
2. Hayajneh, T., Doomun, R., Almashaqbeh, G., Mohd, B.J., 2013. An energy-efficient and security aware route selection protocol for wireless sensornetworks. Secur. Commun. Netw., http://dx.doi.org/10.1002/sec.915.
3. Lasla, N., Derhab, A., Ouadjaout, A., Bagaa, M., Challal, Y., 2014. SMART: secure mlti-paths routing for wireless sensor networks. In: Ad-hoc,Mobile, and Wireless Networks, Lecture Notes in Computer Science, vol. 8487, pp. 332–345.
4. Fouchal, H., Hunel, P., Ramassamy, C., 2014. Towards efficient deployment of wireless sensor networks. Secur. Commun. Netw., http://dx.doi.org/10.1002/sec.1059.

5. Yu, N., Zhang, L., Ren, Y., 2013. A novel D–S based secure localization algorithm for wireless sensor networks. Secur. Commun. Netw.,http://dx.doi.org/10.1002/sec.909.
6. Mary Anita, E.A., Geetha, R., Kannan, E., 2015. A novel hybrid key management scheme for establishing secure communication in wireless sensornetworks. Wirel. Pers. Commun., http://dx.doi.org/10.1007/s11277-015-2290-9.
7. Pooja, Chauhan R. K., 2020. Triple phase hybrid cryptography technique in a wireless sensor network, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2019.1710342.
8. Maliberan Esmael V., 2019. Modified SHA1: A Hashing Solution to Secure Web Applications through Login Authentication. International Journal of Communication Networks and Information Security (IJCNIS), vol. 11(1), pp. 36-41.
9. Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., El-Ebiary, Y. A. B., Nafi, N. S., Rodriguez, R. C., Vargas, D. E., 2021. Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications. Complexity, doi: https://doi.org/10.1155/2021/5540296.
10. Yaksic, V. O. C., 2003. A study on hash functions for cryptography. Global Information Assurance Certification Paper.
11. Bentahar, A., Meraoumia, A., Bradji, L., Bendjenna, H., 2021. Sensing as a service in Internet of Things: Efficient authentication and key agreement scheme. Journal of King Saud University-Computer and Information Sciences.
12. Khari, M., Garg, A. K., Gandomi, A.H., Gupta, R., Patan, R., Balusamy, B., 2019. Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS. pp. 1-8.
13. Dobraunig C., Eichlseder, M., Mendel, F., Schlaffer, M., 2021. ASCON v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology. 34:33. Doi: https://doi.org/10.1007/s00145-021-09398-9.
14. Langrehr, R., Pan, J., 2020. Tightly Secure Hierarchical Identity-Based Encryption. Journal of Cryptology, 33: 1781-1821. Doi: https://doi.org/10.1007/s00145-020-09356-x.
15. Devi, V. A., Kalaivani, V., 2020. Hybrid cryptosystem in wireless body area networks using message authentication code and modified and enhanced lattice-based cryptography (MAC-MELBC) in healthcare applications. Concurrency Computat Pract Exper. 2021;33:e6132. Doi: https://doi.org/10.1002/cpe.6132.
16. Rizk, R., Alkady, Y., 2015. Two-phase hybrid cryptography algorithm for wirelesssensor networks. Journal of Electrical Systems and Information Technology 2 (2015) 296–313. Doi: http://dx.doi.org/10.1016/j.jesit.2015.11.005.
17. Subasree, S., Sakthivel, N.K., 2010. Design of a new security protocol using hybrid cryptography algorithms. IJRRAS 2 (2), 95–103.
18. Kumar, N., 2012. A Secure Communication Wireless Sensor Networks Through Hybrid (AES+ECC) Algorithm, vol. 386. von LAP LAMBERTAcademic Publishing.
19. Ren, W., Miao, Z., 2010. A hybrid encryption algorithm based on DES and RSA in bluetooth communication. In: Proceedings of the 2nd InternationalConference on Modeling, Simulation and Visualization Methods, China, pp. 221–225.
20. Ramaraj DE, Karthikeyan S, Hemalatha M., 2009. A design of security protocol using hybrid encryption technique (AES- Rijndael and RSA). Int J. Comput Internet Manag. 17(1):78–86.
21. Bhole D,Mote A, Patil P. R., 2016 A new security protocol using hybrid cryptography algorithms. International Journal of Computer Sciences and Engineering. 4(2):18–22.
22. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 50.
23. Selvam, R., & Senthilkumar, A. (2014, February). Cryptography based secure multipath routing protocols in wireless sensor network: a survey. In 2014 International Conference on Electronics and Communication Systems (ICECS) (pp. 1-5). IEEE.
24. Ashrif, F. F., Sundararajan, E. A., Ahmad, R., Hasan, M. K., & Yadegaridehkordi, E. (2023). Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. Journal of Network and Computer Applications, 103759.
25. Yang, Z., Li, L., Gu, F., Ling, X., & Hajiee, M. (2022). TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks. Internet of Things, 20, 100627.
26. Nwokoye, C. H., & Madhusudanan, V. (2022). Epidemic models of malicious-code propagation and control in wireless sensor networks: an indepth review. Wireless Personal Communications, 125(2), 1827-1856.
27. Alimoradi, P., Barati, A., & Barati, H. (2022). A hierarchical key management and authentication method for wireless sensor networks. International journal of communication systems, 35(6), e5076.
28. Naresh, V. S., Allavarpu, V. D., & Reddi, S. (2022). Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN. The Journal of Supercomputing, 1-25.

29. Rana, S., Parast, F. K., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. Journal of Information Security and Applications, 78, 103607.
30. Alshrif, F. F., Sundararajan, E. A., Ahmad, R., & Alkhatib, Y. (2021, October). New Framework for Authentication and key Establishment to Secure 6LoWPAN Networks. In 2021 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 1-6). IEEE.
31. Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers. Sensors, 23(18), 7678.
32. da Rocha, H., Caruso, P., Pereira, J., Serra, P., & Espirito Santo, A. (2023). Discussion on Secure Standard Network of Sensors Powered by Microbial Fuel Cells. Sensors, 23(19), 8227.
33. Adil, M., Menon, V. G., Balasubramanian, V., Alotaibi, S. R., Song, H., Jin, Z., & Farouk, A. (2022). Survey: Self-Empowered Wireless Sensor Networks Security Taxonomy, Challenges and Future Research Directions. IEEE Sensors Journal.
34. Basit, A., Nizam, I., Goh, R., Sethumadhavan, S., Hanif, N. R., Hassan, Z., & Mohd Aini, A. (2023). Residents' satisfaction of property management mobile applications: a study in the context of strata property in Kuala Lumpur, Malaysia. Property Management, 41(5), 766-782.
35. Osamy, W., Khedr, A. M., Salim, A., El-Sawy, A. A., Alreshoodi, M., & Alsukayti, I. (2022). Recent Advances and Future Prospects of Using AI Solutions for Security, Fault Tolerance, and QoS Challenges in WSNs. Electronics, 11(24), 4122.
36. Tyagi, H., Kumar, R., & Pandey, S. K. (2023). A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions. High-Confidence Computing, 100127.
37. Nyangaresi, V. O., & Yenurkar, G. K. (2023). Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing, 100178.
38. Goyat, R., Kumar, G., Saha, R., & Conti, M. (2023). Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities. Cluster Computing, 1-17.
39. Shukla, A., Tripathi, S., Sajwan, M., & Singh, D. (2024). SEE2PK: Secure and energy efficient protocol based on pairwise key for hierarchical wireless sensor network. Peer-to-Peer Networking and Applications, 1-21.
40. Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A Scalable Blockchain-based Framework for Efficient IoT Data Management Using Lightweight Consensus.
41. Perera, C., Qin, Y., Estrella, J. C., Reiff-Marganiec, S., & Vasilakos, A. V. (2017). Fog computing for sustainable smart cities: A survey. ACM Computing Surveys (CSUR), 50(3), 1-43.
42. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, 100, 325-343.
43. Wong, W. K., Cheung, D. W. L., Kao, B., & Mamoulis, N. (2009, June). Secure kNN computation on encrypted databases. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data (pp. 139-152).
44. Castelluccia, C., Mykletun, E., & Tsudik, G. (2005, July). Efficient aggregation of encrypted data in wireless sensor networks. In The second annual international conference on mobile and ubiquitous systems: networking and services (pp. 109-117). IEEE.
45. Rawat, A. S., Koyluoglu, O. O., Silberstein, N., & Vishwanath, S. (2013). Optimal locally repairable and secure codes for distributed storage systems. IEEE Transactions on Information Theory, 60(1), 212-236.
46. Koyluoglu, O. O., Koksal, C. E., & El Gamal, H. (2012). On secrecy capacity scaling in wireless networks. IEEE Transactions on Information Theory, 58(5), 3000-3015.
47. Lin, C. H., Hu, G. H., Chan, C. Y., & Yan, J. J. (2021). Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm. Applied Sciences, 11(3), 1329.
48. Rani, N., Sharma, S. R., & Mishra, V. (2022). Grayscale and colored image encryption model using a novel fused magic cube. Nonlinear Dynamics, 108(2), 1773-1796.
49. Sakran, H., Shokair, M., Nasr, O., El-Rabaie, S., & El-Azm, A. A. (2012). Proposed relay selection scheme for physical layer security in cognitive radio networks. Iet Communications, 6(16), 2676-2687.
50. Mou, C., Xu, Y., Song, J., Zhao, C., Ghanem, B., & Zhang, J. (2023). Large-capacity and flexible video steganography via invertible neural network. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 22606-22615).
51. Bellare, M., & Kohno, T. (2004). Hash function balance and its impact on birthday attacks. In Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23 (pp. 401-418). Springer Berlin Heidelberg.
52. DiLuoffo, V., Michalson, W. R., & Sunar, B. (2018). Robot Operating System 2: The need for a holistic security approach to robotic architectures. International Journal of Advanced Robotic Systems, 15(3), 1729881418770011.

53. Zaman, I. U., Lopez, A. B., Al Faruque, M. A., & Boyraz, O. (2018). Physical layer cryptographic key generation by exploiting PMD of an optical fiber link. Journal of Lightwave Technology, 36(24), 5903-5911.
54. Wang, K., Yuan, L., Miyazaki, T., Chen, Y., & Zhang, Y. (2018). Jamming and eavesdropping defense in green cyber–physical transportation systems using a Stackelberg game. IEEE Transactions on Industrial Informatics, 14(9), 4232-4242.
55. Altarawneh, A., Sun, F., Brooks, R. R., Hambolu, O., Yu, L., & Skjellum, A. (2021). Availability analysis of a permissioned blockchain with a lightweight consensus protocol. Computers & Security, 102, 102098.
56. Tong, Q., Miao, Y., Weng, J., Liu, X., Choo, K. K. R., & Deng, R. H. (2022). Verifiable fuzzy multi-keyword search over encrypted data with adaptive security. IEEE Transactions on Knowledge and Data Engineering, 35(5), 5386-5399.
57. Upadhyay, D., Zaman, M., Joshi, R., & Sampalli, S. (2021). An efficient key management and multi-layered security framework for SCADA systems. IEEE Transactions on Network and Service Management, 19(1), 642-660.
58. Wu, W., Parampalli, U., Liu, J., & Xian, M. (2019). Privacy preserving k-nearest neighbor classification over encrypted database in outsourced cloud environments. World Wide Web, 22, 101-123.
59. Wang, G., Yu, J., & Xie, Q. (2012). Security analysis of a single sign-on mechanism for distributed computer networks. IEEE Transactions on Industrial Informatics, 9(1), 294-302.
60. Guo, Z., Zhang, H., Sun, C., Wen, Q., & Li, W. (2018). Secure multi-keyword ranked search over encrypted cloud data for multiple data owners. Journal of Systems and Software, 137, 380-395.
61. Zhu, L., Zhang, C., Xu, C., Liu, X., & Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. IEEE Access, 6, 19025-19033.
62. Su, S., Teng, Y., Cheng, X., Xiao, K., Li, G., & Chen, J. (2015). Privacy-preserving top-k spatial keyword queries in untrusted cloud environments. IEEE Transactions on Services Computing, 11(5), 796-809.
63. Shyla, S. I., & Sujatha, S. S. (2022). Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-13.
64. Zhang, C., Xu, C., Zhu, L., Li, Y., Zhang, C., & Wu, H. (2020). An efficient and privacy-preserving truth discovery scheme in crowdsensing applications. Computers & Security, 97, 101848.
65. AbuTaha, M., Farajallah, M., Tahboub, R., & Odeh, M. (2011). Survey paper: cryptography is the science of information security.