EasyChair Preprint

№ 6823

The Status, Challenges, and Future Trends of Advanced Crypto Algorithms for Wireless Network Security: an Overview

Rana Kaabi, Hassan Fakhruldeen and Karrar Alhamami

October 10, 2021

The status, challenges, and future trends of advanced crypto algorithms for wireless network security: An Overview

Rana Abbas Al-Kaabi[1*], Hassan Falah Fakhruldeen[2], and karrar ezzulddin kareem alhamami[3]

College of Information Technology, University of Babylon, Hilla, Iraq.
ranaa.net.msc@student.uobabylon.edu.iq

Department of Electrical Engineering, Faculty of Engineering, University of Kufa, Kufa, Najaf, Iraq.
Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.
Hassan.fakhruldeen@gmail.com

College of Mathematics and Computer, University of Kufa, Kufa, Najaf, Iraq.
kalhamamy1@gmail.com

Abstract. Modern applications, particularly real-time applications, require high-speed end-to-end transmission, which regularly conflicts with the requirements of confidentiality and security. Advanced Crypto is one of the most promising research areas in cryptography since it is considered fast in encryption processing, resistant to attacks and low in resource requirements. The main reasons for adopting Advanced Crypto for smart power constrained devices are the need for efficient end-to-end communication and adoptability in resource-constrained smart devices. Generally, any cryptographic design should take into considerations the tradeoff between security, cost and performance. The performance measurements include power, energy consumption, latency and throughput. Security requirements, on the other hand, aim to maintain an acceptable level of secrecy and privacy of the system.

Keywords: Advanced Crypto, Asymmetric, Symmetric ,Security, Resource-constrained.

1 Introduction

Several emerging areas of information and communication technology (ICT) require interconnected devices like Internet of Things (IoT) and sensor networks. IoT and smart applications are growing rapidly and are commonly accessed through smartphones. Currently, more and more smart devices are daily connected to the internet, such as smartphones, smart TVs, video game consoles and even most of the home devices like refrigerators and air-conditioners [1]. All of these tools have resource limitations because to their low processing power, short battery life, small screen size, poor memory capacity, and limited storage. Smart applications, such as IoT, face numerous issues and threats, including dealing with massive volumes of data, computing power, energy consumption, and addressing security and privacy issues [2].

Security and privacy are fundamental requirements for any application, especially smart applications. The current modern standard cryptographic algorithms were originally designed for traditional desktop/server implementations and many of them consume an unacceptable amount of system resources (computation power, RAM, storage, etc.) and are not suitable for resource-constrained devices.[3]. Therefore, there is a need for lightweight cryptography (LWC) algorithms that suit such resource-constrained devices [4].

LWC is one of the most promising research areas in cryptography since it is considered fast in encryption processing, resistant to attacks and low in resource requirements. There are no strict properties needed in order to classify an encryption algorithm as an LWC [5]. According to the National Institute of Standards and Technology (NIST), the main reasons for adopting LWC for smart power constrained devices are the need for efficient end-to-end communication and adoptability in resource-constrained smart devices [6].

Generally, any cryptographic design should take into considerations the tradeoff between security, cost and performance. The performance measurements include power, energy consumption, latency and throughput. Security requirements, on the other hand, aim to maintain an acceptable level of secrecy and privacy of the system. Cryptography, which is part of security, is divided into symmetric and asymmetric cryptography[7].

Traditional symmetric and asymmetric algorithms are not suitable for constrained devices while lightweight cryptographic algorithms are the best choice [8]. Some of the candidate applications for the LWC algorithms include wireless sensor network (WSN), radio-frequency identification, wireless body area network (WBAN), IoT, smart cards, embedded systems, smart systems, etc. [9]. These applications support dissimilar devices in heterogeneous environments with minimum human intervention. For example, IoT devices communicate with minimum or no human intervention, a fact that represents a new challenge to the IoT system by both exposing many security attacks as well as gaining unauthorized device access by the attacker device. This may essentially result in severe system damages. Moreover, some IoT implementations are cloud-based applications which have many security issues and challenges [10].

System performance based on lightweight algorithm

- Lightweight(computation power) as the minimum required number of iterations[12].
- Flexibility.
- Simple hardware and software implementation.
- Low error propagation [13].

These changes help speed the encryption and decryption process and simplify the hardware implementations associated with them[14].

2 Literature Survey

In [15] also evaluates a cryptographic algorithm (RC5). The Blowfish and DES block cipher algorithms were compared using the C# program. Using a set of input files, a comparison of RC5, Blowfish, and DES is performed, and the encryption and decryption times are evaluated. According to the results, RC5 is 1.54 times faster than Blowfish and 2.57 times faster than DES. The results also show that the Blowfish

algorithm's performance is inversely proportional to key size; as key size increases, so does performance, and vice versa. In terms of resource utilization, RC5 uses more memory than Blowfish and DES, while all three algorithms use roughly the same amount of CPU. As a result, the RC5 block cipher algorithm is both faster and simpler than Blowfish and DES. When a high encryption rate is required, RC5 is beneficial [16].

AES, DES, 3DES, RC6, Blowfish, and RC2 are the algorithms[17] used. The simulation results enable several conclusions to be drawn, and it is discovered that Blow-fish performs the best of all algorithms. Following that, in terms of power and time consumption, RC6 is the best algorithm. RC2 is also the worst approach in terms of CPU load of all algorithms because its time consuming factor causes a high workload on the CPU [18].

Stream cipher and block cipher are two common cipher techniques. Both were pretty thoroughly studied and implemented in current cipher systems [19] [20]. Stream cipher is a symmetric key cipher technique which involves combining some plaintext data digits with a digit stream of pseudo-random cipher known as key stream. In stream cipher, the cipher text stream digits are generated by encrypting each digit of the plaintext separately with the specified digit of the key stream. The digits' encryptions are determined by the cipher state at the time. As a result, it is known as a state cipher. Exclusive-or (XOR) is used as a stream cipher function.

The TinySec Protocol, the first full implementation of a secure architecture at the data link layer for WSN, is proposed in [22]. This solution includes two levels of security: message authentication with data encryption (TinySec-EA) and message authentication without data encryption (TinySec-EA) (TinySec-Auth). TinySec, such as SPINS, uses common cryptographic methods to secure message integrity and privacy. Tinysec's creators believe that the Skipjack algorithm [23] is better for WSN than RC5 (algorithm used by SPINS).

SPINS is a proposed set of security building blocks in [24]. It is optimized for environments with limited resources and wireless connection. SPINS is built on two secure pillars: SNEP and TESLA. SNEP utilizes a shared counter between the two communicating parties to calculate encryption and a message authentication code (MAC) in order to offer data secrecy, semantic security, data integrity, two-party data authentication, replay protection, and weak message freshness.

In [25] suggest micro-PKI (Public Key Infrastructure Micro), a simplified version of standard PKI, as a method for WSN. The base station contains two keys: one public and one private. The network nodes utilize the public key to authenticate the base station, while the base station uses the private key to decrypt data transferred from the nodes. The base station's public key is saved in all nodes prior to deployment. Two forms of authentication are included in the authors' scheme (HandShake). Between a network node and the base station, the first type of authentication takes place. The node generates a symmetric session key, which it encrypts with the client's public key.

in [26] proposed TinyPK, a method for establishing a secret key between two nodes in a WSN based on the usage of public keys and the Diffie-Hellman principle. TinyPK signs the public keys of nodes with a trustworthy authority. Before deployment, the CA key is pre-distributed to all nodes so they may verify key neighbors. The RSA algorithm requires a lot of time and energy from the nodes. As a result,

fundamental operations may take a few seconds, reducing network lifetime and reducing reactivity.

The PKKE and CBKE protocols proposed by Zigbee using the identity of nodes in their method of key establishment. The goal is to use these identities to create a single shared key between each pair of nodes in a network. However, the creation of the shared key is performed with interactions between the two nodes. It means, methods require sending and receiving multiple messages on both sides before the creation of the key. To save power nodes that want to share a secret and those intermediate nodes, several methods have been proposed to remove these interactions. These methods are known in the field of cryptography as the ID-NIKDS [27] (Identity-Based Non-Interactive Key Distribution Scheme).

In [28] introduced the C4W technique, which focuses on the identity of nodes to calculate public keys. The public keys of other nodes can also be calculated by the nodes themselves using their identities. What could possibly take the place of a certificate? The nodes and base station are supplied with their own keys (private / public key ECC) and public information on the network nodes before deployment. Without utilizing certificates, the C4W technique leverages the Diffie-Hellman key exchange concept to produce a single shared key between two nodes.

Main Topics of the Seminar

Information security refers to the protection of data and its critical components, such as the software and hardware that process, store, and transfer it. In today's digital environment, cryptography is extremely crucial. To suit the varied requirements emerging from applications, many cryptographic algorithms have been created [29][30].

The mathematical function used for encryption and decryption is defined as a cryptographic algorithm, usually known as a cipher. In general, there are two functions that are related: one for encryption and the other for decryption [31]. Encryption/decryption prevents an adversary from gaining access to information. Encryption/decryption is a security strategy in which cipher algorithms are used in conjunction with a secret key to encrypt data, rendering it unintelligible if intercepted [32]. Type, complexity, and attack are three properties of encryption algorithms that were taken into account when developing metrics [33].

Strongest Advanced Data Encryption Algorithms [34], [35], [36]

1) Triple Data Encryption Standard (TripleDES)
2) Blowfish Encryption Algorithm
3) Twofish Encryption Algorithm
4) Advanced Encryption Standard (AES)
5) IDEA Encryption Algorithm
6) MD5 Encryption Algorithm
7) HMAC Encryption Algorithm

8) RSA Security

1) Triple Data Encryption Standard (DES)

It is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. ... Three keys are referred to as bundle keys with 56 bits per key[37].

2) The Blowfish algorithm

It is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. It works for key size of 256 and 448 bits also. It is related to AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish[38].

3) Twofish Encryption Algorithm

It is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. ... The actual encryption key is one half of an n-bit key, and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes)[39].

4)Advanced Encryption Standard (AES)

The Advanced Encryption Standard, also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology[40].

5) IDEA Encryption Algorithm

International Data Encryption Algorithm (IDEA) is a once-proprietary free and open block cipher that was once intended to replace Data Encryption Standard (DES). Once called Improved Proposed Encryption Standard (IPES)I, DEA is a minor revision to the Proposed Encryption Standard (PES)[41].

6) MD5 Encryption Algorithm

The MD5 message-digest algorithm is a popular hash function that generates a 128-bit hash value. Although MD5 was originally intended to be used as a cryptographic hash function, it has been discovered to have numerous flaws[42].

7) HMAC Encryption Algorithm

HMAC is a specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message[43].

8) RSA Encryption Algorithm

The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone[44].

- Challenges:

Choosing of adequate cryptographic method is relied on the sensor nodes processing capabilities; therefore, there is no combined or unified solution that fit all WSNs as one of the most important application of wireless network[45].

As there are many constraints that are related to WSNs such as computation capability, storage, etc.; therefore, any design that is presented for WSNs security services must adequately satisfy these constraints.

Mobility on Wireless Networks brings up many challenges to Wireless Networks security[46].

Advanced Cryptography is an adequate security solution for many scenarios of resource constraint devices like WSNs devices but still needs more enhancements to reduce the overheads to an acceptable rate that fit particularities and constraints[47].

3 Current Status

There are many current status research direction in this work based on :

- Current status of researcher in advanced crypto algorithms for wireless networks directed on :
- Identity-based encryption transformation for flexible sharing of encrypted data in public cloud[48]
- Novel crypto for data security in fog computing[49]
- Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks[50]
- Advanced Encryption Standard (AES) secure replacement for DES[51]
- Modified RSA Using Triple Keys Based Encryption/Decryption[52]
- Energy Proficient Hybrid Secure Scheme for Wireless Sensor Networks[53]
- QoS aware trust based routing algorithm for wireless sensor networks[54]
- Blockchain mechanism and symmetric encryption in a wireless sensor network[55]

4 Still Open Problems

- lack of Wireless network scalability requirements[56]
- ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things[57]
- Design of a dynamic key management plan for intelligent building energy management system based on wireless sensor network and block chain technology[58]

- Trusted Model for IoT enabled cancer prediction system to enhance the authentication and security using cloud computing[59]

5 Future Trends

- FPGA implementations for data encryption and decryption via concurrent and parallel computation[60]
- Analysis of using blockchain to protect the privacy of drone big data[61]
- A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine[62]
- Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems[63]
- Lightweight blockchain assisted secure routing of swarm UAS networking[64]

6 Conclusion

Data security is a critical issue in every arena, as data is transmitted across an unreliable network. Numerous techniques to data protection have been offered; nonetheless, cryptography is one of the most dependable approaches. Cryptographic techniques aid in the transformation of the original data into unintelligible data. Numerous new sectors involve the interconnection and communication of very limited devices in order to execute certain tasks. Today, the Internet of Things (IoT) enables a large number of low-resource and resource-constrained devices to communicate, compute, and make decisions within a communication network. There are numerous obstacles and issues in heterogeneous IoT systems, such as device power consumption, limited battery capacity, memory space, performance cost, and security. It is critical that the advanced encryption algorithm chosen be both robust and lightweight.

References

1. Saraf, S. B., & Gawali, D. H. (2017, May). IoT based smart irrigation monitoring and controlling system. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 815-819). IEEE.
2. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. big data and cognitive computing, 2(2), 10.
3. Al-Omari, A. H. (2019). Lightweight dynamic crypto algorithm for next internet generation. Engineering, Technology & Applied Science Research, 9(3), 4203-4208.
4. Manifavas, C., Hatzivasilis, G., Fysarakis, K., & Rantos, K. (2013). Lightweight cryptography for embedded systems–a comparative analysis. In Data Privacy Management and Autonomous Spontaneous Security (pp. 333-349). Springer, Berlin, Heidelberg.
5. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access.

6. Moura, J., & Hutchison, D. (2020). Fog computing systems: State of the art, research issues and future trends, with a focus on resilience. Journal of Network and Computer Applications, 102784.
7. Mao, B., Kawamoto, Y., & Kato, N. (2020). AI-based joint optimization of QoS and security for 6G energy harvesting internet of things. IEEE Internet of Things Journal, 7(8), 7032-7042.
8. Manifavas, C., Hatzivasilis, G., Fysarakis, K., & Rantos, K. (2013). Lightweight cryptography for embedded systems–a comparative analysis. In Data Privacy Management and Autonomous Spontaneous Security (pp. 333-349). Springer, Berlin, Heidelberg.
9. Wu, Q., Ding, G., Xu, Y., Feng, S., Du, Z., Wang, J., & Long, K. (2014). Cognitive internet of things: a new paradigm beyond connection. IEEE Internet of Things Journal, 1(2), 129-143.
10. Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.
11. Shah, A., & Engineer, M. (2019). A survey of lightweight cryptographic algorithms for iot-based applications. In Smart innovations in communication and computational sciences (pp. 283-293). Springer, Singapore.
12. Shun, J., & Blelloch, G. E. (2013, February). Ligra: a lightweight graph processing framework for shared memory. In Proceedings of the 18th ACM SIGPLAN symposium on Principles and practice of parallel programming (pp. 135-146).
13. Dalton, M., Kannan, H., & Kozyrakis, C. (2007). Raksha: a flexible information flow architecture for software security. ACM SIGARCH Computer Architecture News, 35(2), 482-493.
14. Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., & Piuri, V. (2003). Error analysis and detection procedures for a hardware implementation of the advanced encryption standard. IEEE transactions on Computers, 52(4), 492-505.
15. Sharafi, M., Fotouhi-Ghazvini, F., Shirali, M., & Ghassemian, M. (2019). A low power cryptography solution based on chaos theory in wireless sensor nodes. IEEE Access, 7, 8737-8753.
16. Saraiva, D. A., Leithardt, V. R. Q., de Paula, D., Sales Mendes, A., González, G. V., & Crocker, P. (2019). Prisec: Comparison of symmetric key algorithms for iot devices. Sensors, 19(19), 4312.
17. [ÖZDEN, S., & KILIÇ, F. (2019). Performance evaluation of GSA, SOS, ABC and ANN algorithms on linear and quadratic modelling of eggplant drying kinetic. Food Science and Technology, (AHEAD).
18. Advani, N., Rathod, C., & Gonsai, A. M. (2019). Comparative study of various cryptographic algorithms used for text, image, and video. In Emerging Trends in Expert Applications and Security (pp. 393-399). Springer, Singapore.
19. Kuznetsov, O., Potii, O., Perepelitsyn, A., Ivanenko, D., & Poluyanenko, N. (2019). Lightweight stream ciphers for green IT engineering. In Green IT Engineering: Social, Business and Industrial Applications (pp. 113-137). Springer, Cham.
20. Liu, T., Wang, Y., Li, Y., Tong, X., Qi, L., & Jiang, N. (2020). Privacy Protection Based on Stream Cipher for Spatiotemporal Data in IoT. IEEE Internet of Things Journal, 7(9), 7928-7940.
21. Jiao, L., Hao, Y., & Feng, D. (2020). Stream cipher designs: a review. Science China Information Sciences, 63(3), 1-25.
22. Perković, T., Čagalj, M., & Kovačević, T. (2019). LISA: Visible light based initialization and SMS based authentication of constrained IoT devices. Future Generation Computer Systems, 97, 105-118.
23. Kumar, R., Tripathi, S., & Agrawal, R. (2020). An analysis and comparison of security protocols on wireless sensor networks (WSN). In Design Frameworks for Wireless Networks (pp. 3-21). Springer, Singapore.
24. Stoyanov, B., & Stoyanov, B. (2020). BOOST: Medical Image Steganography Using Nuclear Spin Generator. Entropy, 22(5), 501.
25. Xin, R., Kar, S., & Khan, U. A. (2020). Gradient tracking and variance reduction for decentralized optimization and machine learning. arXiv preprint arXiv:2002.05373.
26. Rakesh, B., & Sultana, H. P. (2021). A novel methodology for secure group communication in Internet of Things. Materials Today: Proceedings.
27. Singh, S., & Saini, H. S. (2021). Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN. Wireless Personal Communications, 118(1), 789-814.
28. Mahmud, A. S. M. (2018). A real-time demand response pricing model for the smart grid.

29. Gordon, D. E., Jang, G. M., Bouhaddou, M., Xu, J., Obernier, K., White, K. M., ... & Krogan, N. J. (2020). A SARS-CoV-2 protein interaction map reveals targets for drug repurposing. Nature, 583(7816), 459-468.
30. Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), 102397.
31. Englander, I., & Wong, W. (2021). The architecture of computer hardware, systems software, and networking: An information technology approach. John Wiley & Sons.
32. Winkel, M. (1984). Microprocessors that protect object code: An investigation of their architectures and potential for inhibiting software piracy (Doctoral dissertation, University of Wyoming).
33. Hossain, M. A., Hossain, M. B., Uddin, M. S., & Imtiaz, S. M. (2016). Performance analysis of different cryptography algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3).
34. Verma, O. P., Agarwal, R., Dafouti, D., & Tyagi, S. (2011, April). Notice of Violation of IEEE Publication Principles: Peformance analysis of data encryption algorithms. In 2011 3rd International Conference on Electronics Computer Technology (Vol. 5, pp. 399-403). IEEE.
35. Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). Journal of Research of the National Institute of Standards and Technology, 106(3), 511.
36. Shahbazi, K., Eshghi, M., & Mirzaee, R. F. (2017). Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5. Engineering science and technology, an international journal, 20(4), 1308-1317.
37. Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In 2005 international Conference on information and communication technologies (pp. 84-89). IEEE.
38. Rogaway, P., Bellare, M., & Black, J. (2003). OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security (TISSEC), 6(3), 365-403.
39. Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 19-22.
40. Basu, S. (2011). International data encryption algorithm (idea)–a typical illustration. Journal of global research in Computer Science, 2(7), 116-118.
41. Pittalia, P. P. (2019). A Comparative Study of Hash Algorithms in Cryptography. International Journal of Computer Science and Mobile Computing, 8(6), 147-152.
42. Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A. K., Molnar, D., Osvik, D. A., & de Weger, B. (2008). MD5 considered harmful today, creating a rogue CA certificate. In 25th Annual Chaos Communication Congress (No. CONF).
43. Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.
44. Jorstad, N. D., & Landgrave, T. S. (1997, January). Cryptographic algorithm metrics. In 20th National Information Systems Security Conference (pp. 1-38).
45. Sen, J. (2010). A survey on wireless sensor network security. arXiv preprint arXiv:1011.1529.
46. [46] Kulkarni, R. V., Förster, A., & Venayagamoorthy, G. K. (2010). Computational intelligence in wireless sensor networks: A survey. IEEE communications surveys & tutorials, 13(1), 68-96.
47. Kamgueu, P. O., Nataf, E., & Ndie, T. D. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. Computer Communications, 120, 10-21.
48. Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., & Attia, R. (2018). Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. Computer Networks, 133, 141-156.
49. Murugesan, A., Saminathan, B., Al‐Turjman, F., & Kumar, R. L. (2020). Analysis on homomorphic technique for data security in fog computing. Transactions on Emerging Telecommunications Technologies, e3990.

50. Al-Ahdal, A. H. (2021). Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 133-143.
51. El Batouty, A. S., Farag, H. H., Mokhtar, A. A., El-Badawy, E. S. A., & Aly, M. H. (2020). Improvement of Radio Frequency Identification Security Using New Hybrid Advanced Encryption Standard Substitution Box by Chaotic Maps. Electronics, 9(7), 1168.
52. Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., ... & Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International journal of distributed sensor networks, 16(6), 1550147720925772.
53. Yuvaraju, M., & Pranesh, K. A. (2021). Energy Proficient Hybrid Secure Scheme for Wireless Sensor Networks. Wireless Personal Communications, 117(2), 747-767.
54. [54] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110(4), 1637-1658.
55. Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., & Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors, 20(10), 2798.
56. Abadal, S., Mestres, A., Torrellas, J., Alarcón, E., & Cabellos-Aparicio, A. (2018). Medium access control in wireless network-on-chip: A context analysis. IEEE Communications Magazine, 56(6), 172-178.
57. Majumder, S., Ray, S., Sadhukhan, D., Khan, M. K., & Dasgupta, M. (2021). ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. Wireless Personal Communications, 116(3), 1867-1896.
58. Jia, C., Ding, H., Zhang, C., & Zhang, X. (2021). Design of a dynamic key management plan for intelligent building energy management system based on wireless sensor network and blockchain technology. Alexandria Engineering Journal, 60(1), 337-346.
59. Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301.
60. Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301.
61. Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. IEEE Network, 35(1), 44-49.
62. Pavithran, P., Mathew, S., Namasudra, S., & Lorenz, P. (2021). A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine. Computers & Security, 104, 102160.
63. Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 1-38.
64. Wang, J., Liu, Y., Niu, S., & Song, H. (2021). Lightweight blockchain assisted secure routing of swarm UAS networking. Computer Communications, 165, 131-140.