

# A hybrid lightweight security approach in internet of things for healthcare application

Ameer Saad Kadhim<sup>1</sup>, Ali Haider Alazam<sup>2</sup>, Noor Fahem Sahib<sup>3</sup>

<sup>1</sup>Department of Computer, Babylon Education Directorate (BED), Babylon, Iraq

<sup>2</sup>Department of Medical Physics, Al-Mustaqbal University College, Babylon, Iraq

<sup>3</sup>Department of Food Science and Technology, College of Food Science, Al-Qasim Green University, Babylon, Iraq

## Article Info

### Article history:

Received Jul 16, 2022

Revised Aug 18, 2022

Accepted Sep 4, 2022

### Keywords:

Data security

Healthcare

Internet of things

PRESENT

TEA

## ABSTRACT

The internet of things (IoT) is a rapidly developing area that consists of a globally linked network architecture based on the Internet. The internet of healthcare things (IoHT) is a subset of IoT that comprises of smart healthcare devices that are critical in monitoring, processing, storing, and transferring sensitive data. It is confronted with new issues in terms of data privacy protection. To safeguard healthcare information, this work proposes hybrid lightweight ciphers (PRESENT and TEA) that leverage elliptic curve cryptography (ECC) in the key generation phase. The proposed system evaluated using the main network evaluation parameters as throughput in Kbps, delay in ms, packet loss rate (%). The proposed approach provides secure data transmission of IoT devices based on the used lightweight security algorithms, in addition it provides conserving network performance, improving channel resource usage, network latency is increased due to the security level added by PRESENT and TEA with ECC, and decrease number of loss packets compared without security case study.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Ameer Saad Kadhim

Department of Computer, Babylon Education Directorate (BED)

51001 Babylon, Iraq

Email: ameer.saad@bab.epedu.gov.iq

## 1. INTRODUCTION

The internet of things (IoT) is a model that has gained popularity in recent years [1]. How does it indicate the extent of the interdependence between devices with sensors in our daily lives, such as personal computers, laptops, tablets, many smartphones, and other sensor devices that sense these devices with each other intelligently in order to enable the connection of things anywhere, anytime, and anyone can ideally use these services over the network [2]. It is a new revolution of the internet. Devices can learn about each other, use intelligence to make contextual decisions, and access information collected in many ways [3].

The challenges of providing security in IoT networks include that it is relatively new and has not been much testing of security concepts as a top priority during the product design phase, to that IoT lab is an emerging market. Other steps to build security, which sometimes requires building the system from scratch [4]. A common example is the use of encrypted passwords or thousands that can lead to personal violations if they are not dealt with properly. It is very important that the passwords are very strong, it is difficult to change by hacked and prevent intrusion [5].

Among the other problems facing the IoT is that it is not restricted to resources and does not contain computing resources to implement a strong analysis [6]. Many devices do not accept advanced security features. For example, sensors that are based on simple functional tasks, such as sensors that monitor humidity and temperature, and can't handle it optimally with advanced encryption and other business processes [7]. In addition,

many IoT devices are fielded on a device and left to the end of their lifespan, where security updates or patches rarely upgrade from a company's systems perspective. In addition to upgrading, upgrading and updating devices from the perspective of network systems and leaving it until the end of its life [8].

The internet of health things (IoHT) is a subsection of the IoT that enables remote data exchange from physical activities including monitoring of patients, medication progress, observation, and consultation [9]. IoHT offers connection, integration, computation, and interoperability through a range of sensors, actuators, and controllers, resulting in seamless connectivity and resource efficiency. Because of improvements in telemedicine, telesurgery, and other healthcare applications, streaming has become an important component of IoHT [10]. Transmission of data from apps Interactive multimedia streaming, real-time picture processing, and traffic data created by faulty sensors and vital signs are all enhanced by the IoT in health care [11]. It referring about packet loss, which requires extremely high latency yet can't be avoided. In video streaming applications, jitter can be tolerated, thus low-power devices are sensitive to it. Some are tolerant of data delivery delays but not jitter, which has distinct quality of service (QoS) requirements in terms of delay, packet loss, and throughput [12].

The majority of today's data security and encryption technologies in IoT in healthcare are computationally expensive, which has an influence on energy consumption, which is a very influential factor in energy-specific sensors [13]. Traditional encryption solutions are not applicable to healthcare IoT applications. It is important to adopt encryption techniques with low computational complexity, less weight, and minimal user authentication requirements, to ensure consumer confidentiality on the IoT now, by relying on lightweight algorithms [14].

The most related works in lightweight algorithms for IoT are presented: radio frequency identification (RFID) systems are vulnerable to a variety of harmful assaults. By developing RFID technology day by day, the hazards are changing as well [15]. Given the nature of RFID tags, it's critical to use a variety of cryptographic algorithms to mitigate security and privacy concerns. Because the execution of these systems would demand a lot of processing power, memory, and resources, modern encryption techniques built for high-end devices are not suited for RFID tags [16].

The DoT technique was proposed in [17] and it was utilized with 64-bit block data using the SPN structure. As a result, it accepts a secret key of 80/128 bits and 31 rounds. Adding subkeys, S-boxes, shifting, permutation bits, and other shifting operations are all part of the round function. DoT employs a four-by-four S-box, with each permutation shifting bit being assigned to a separate fixed table. DoT presupposes a low-power architecture in permutations of bits that don't require a lot of memory and are rapid to execute.

Chandrasekhar *et al.* [18] suggested special licensing procedures based on a group of peers that bridge the gap between encryption and non-encryption techniques. The health care institutions and patient care are the basic components of the system that contribute to the selective and approved exchange of health information for patients. They relied on creating a unique protocol that contributes to the signature of the accreditation agent, on a proprietary hashing algorithm called the hash-based proxy signature technique. The proposed protocol provides the best tool that is proven to be secure in a set of trends in security and overall performance.

An architecture based on attribute based encryption (ABE) has been proposed in [19]. Because emergency access is only brief, it is critical to remove the access permissions that have been granted. Revocation, on the other hand, is a challenging issue in ABE systems and can result in significant cost. The revocation problem of an emergency key was solved using integer values and integer comparisons [20]. They also offered a number characteristic with a data value to describe the emergency key's validity data. Simulations of three situations revealed that the proposed approach may minimize revocation costs and emergency reaction times, implying that it can offer effective and fine-grained access control. A new cloud-based architecture has been suggested in [21] for medical wireless sensor networks and relying on an access control system based on a people-policy encryption method ciphertext policy-(CP-ABE), which allows sophisticated and dynamic security rules to be precisely scalable for simulation data.

A lightweight secure efficient offloading scheduling (LSEOS) metaheuristic model is developed in [22]. It consists of a set of lightweight, secure schedule techniques that have less response time than previous techniques and aims to implement application workflows on the contract in order to reduce system latency and business risks. It has a role in scheduling deadlines using search strategies, the proposed system proved a schedule operational application with 10% safety and 29% delays based on computational results when compared to current delay and safety check strategies. A rest of this article usually follows structure: 1 is introduction, 2 is method, 3 is results and discussion, and 4 is conclusion.

## 2. METHOD

The proposed system has been implemented based on the hybrid lightweight security approach with (PRESENT and TEA) security algorithms for IoT healthcare system with the following specifications showed in Table 1 as the specifics of the environment in which the suggested system was put into practice. Objective modular network testbed (OMNET++) simulation tool has been used to write the C++ code for the proposed

*A hybrid lightweight security approach in internet of things for healthcare application (Ameer Saad Kadhim)*

system. The main aims of the proposed works are to satisfy the following objectives: i) design a robust authentication and light weight encryption approach to deny the IOT attacks and ii) preserving the privacy of patient data, and the proposed system uses robust lightweight encryption in addition to compatibility with low-resource IoT devices. The proposed system implemented with the simulation environment as showed in Figure 1. Figure 2, showed the encapsulated data passed from the actuator to the server. In addition, Table 2 presents the specifications of each network elements which effected on the resource allocation process, with network configuration IP address, network interface, and port number.

Table 1. Environment specifications for the proposed system

Operating systems	windows 7, 32-bit
CPU	Core (TM) I 5-4210U
RAM	4.00 GB
Implementation Tools	OMNET++ 4.6, INET 3.3.0

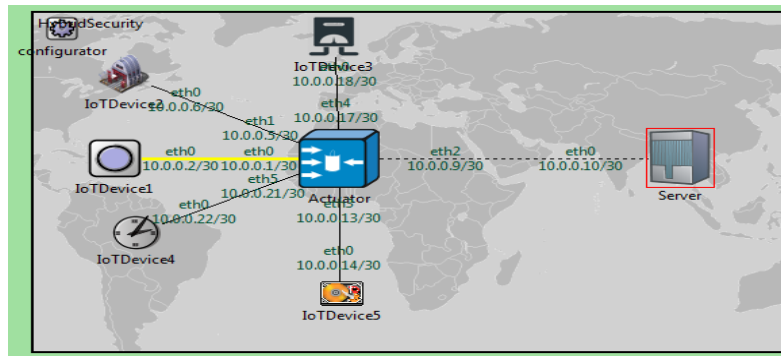


Figure 1. The proposed implementation system in OMNET++ environment

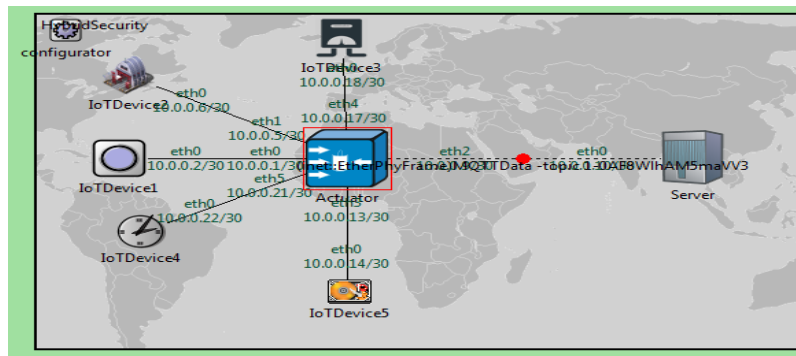


Figure 2. The encapsulated image file upload from the actuator to the server

Table 2. The specification of the IoT healthcare environment

Node IP	The behavior	Network interface
10.0.0.2/30	IoT device 1	eth0-eth0
10.0.0.6/30	IoT device 2	eth0-eth1
10.0.0.18/30	IoT device 3	eth0-eth5
10.0.0.22/30	IoT device 4	eth0-eth7
10.0.0.14/30	IoT device 5	eth0-eth3
10.0.0.1/30	Local gateway (actuator)	eth0
10.0.0.5/30		eth1
10.0.0.9/30		eth2
10.0.0.13/30		eth3
10.0.0.17/30		eth4
10.0.0.21/30		eth5
10.0.0.10/30	Server	eth0-eth2

The main steps of the proposed system explained as follow:

Phase 1: collect dataset using IoT device and then preprocessing.

Phase 2: key generation using elliptic curve cryptography (ECC) with the main steps:

- It is based on the establishment of an anonymous main agreement between the two parties to the communication represented by the first party A and the second party B. It allows the creation of a shared secret key represented elliptic curve public-private key pair both keys are used to ensure the security of the connection.

Phase 3: hybrid lightweight security between PRESENT and TEA algorithms and then encryption data of patients using actuator local gateway device as it provides:

- Before being transferred to the server, data is pre-processed.
  - Filtering data before sending it to the server, since if this isn't done, server services will decrease in terms of speed and accuracy, putting patients receiving direct health care at risk.
- a. In a hybrid lightweight encryption approach, TEA and PRESENT are employed.
- The crypt procedure's start point offset for the key component.
  - For each side, calculate the shift count in bits.
  - The size of the key is specified in 16-bit blocks.
  - The buffer size that will be used to hold the new values throughout the permutation stage.
  - The buffer size used to hold rotated blocks during left-right shifts.
  - The least significant bit (LSB) and most significant bit (MSB) arrived side by side after rotating to the left.
  - The LSB and MSB arrived side by side after rotating to the right.
  - TEA/PRESENT, which makes use of an ECC key generator.
  - The block count will be adjusted after the rotation point for left-right shifts.
  - The offset value of the LSB bits source block during left-right shifts.
  - Construct the encrypted data and add the last subkey to complete the operation. In addition, the proposed system encryption phase showed in Figure 3.

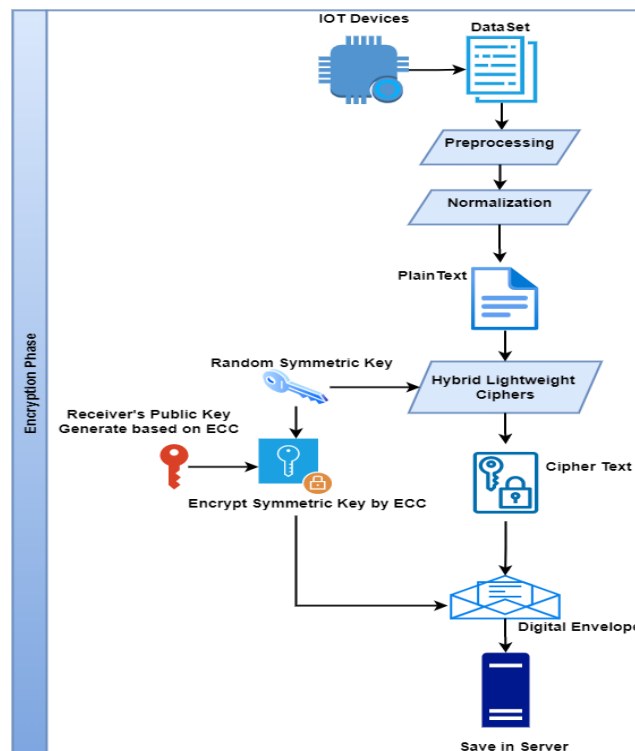


Figure 3. Encryption phase of proposed system

b. Decryption process

- Store the key into buffer to take the existing value constant during the decryption process.
- Create a decryption key using the encryption key.
- The final phase in the encryption process is the first stage of decryption. Add the decryption key that was generated first.

- The primary loop of the PRESENT and TEA decryption algorithms. Decryption of a lightweight hybrid, decryption process showed in Figure 4.

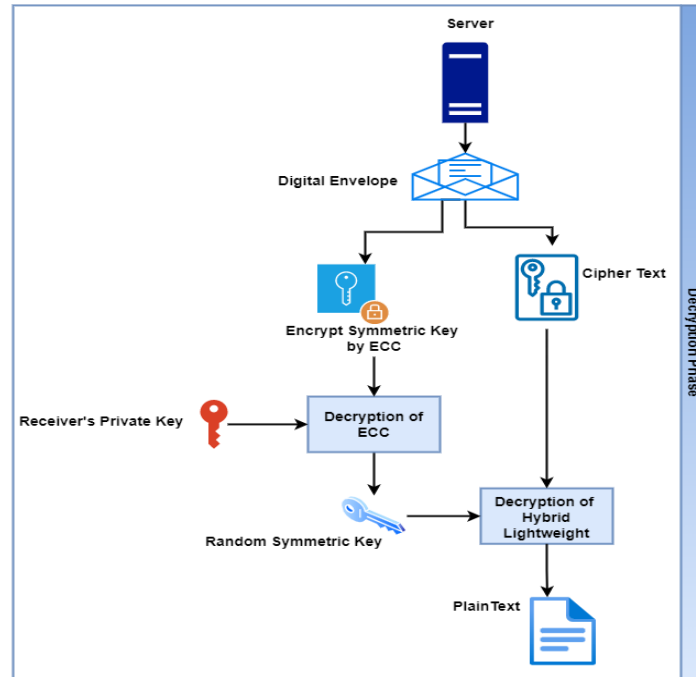


Figure 4. Decryption phase of proposed system

#### Phase 4: evolution of proposal system

The proposed algorithm is evaluated to encrypt files in the form of an image, where many parameters are calculated as follows:

- Payload throughput it measures the average number of payload bytes successfully transferred per unit time  $T$ . It's either all  $B$  bytes go to the actuator, or nothing gets there at all. As a result, we calculate the  $i$ th interval's total number of successfully delivered bytes as the product of  $B$  and  $i$ . In (1), the value of  $I$  shows whether or not the bytes were successfully sent [23]:

$$Payload\ Throughput = \frac{1}{r} \sum_{i=1}^r \frac{B * \delta_i}{T} = \frac{B}{r * T} \sum_{i=1}^r \delta_i \quad (1) [23]$$

$\delta_i=1$  the actuator gets the  $i$ -th message

$\delta_i=0$  the actuator does not get the  $i$ -th message

- At some point during the transfer of data, a packet is lost. This is called packet loss. Packets may be dropped by witches if network switches are overloaded and unable to handle the incoming traffic. The packet loss rate is an indication of the switch's busy state and the path's load state. A path's packet loss rate is computed using (2) [24]:

$$P_{Loss} = \frac{Packet_T - Packet_R}{Packet_T} \quad (2) [24]$$

- The delay time is the amount of time it takes for a packet to go from the sender to the receiver, which explains the delay time simulation parameter for all packets. The following equation is used to calculate it [25]:

$$d_{trans} = L/R \quad (3) [25]$$

the  $D$  represents the time it takes for a packet of data to be transferred and the number of bits per second it transmits [25].

- Channel resource utilization: it represents the maximum utilization of the resources available in a IoT healthcare system [26].

**3. RESULTS AND DISCUSSION**

The propose system results based on the two case studies. The 1<sup>st</sup> is the case of with hybrid lightweight security to provide secure connection among network elements and the 2<sup>nd</sup> is the case of without security system.

**3.1. The 1<sup>st</sup> case study with hybrid lightweight (PRESENT and TEA) security approach**

It is based on the implementing the proposed approach between actuator and server with hybrid lightweight security system to analyze the impact of combining PRESENT with TEA on the used evluation metrics. Table 3 showed the main evluation metrics of the 1st case study. Table 4 showed the channel resources allocation for IoT healthcare sensor network elements of the 1<sup>st</sup> case study.

Table 3. Payload throughput, avg delay, and packet loss rat of hybrid lightweight security approach

Network element	Payload throughput/Kbps (Encapsulated/Decapsulated)		Avg delay/ms	Packet loss rate (%)
	frames/sec sent	Frames/sec received		
Actuator	61.447	58.374	21744.87	3.073
Server	54.726	47.780	24012.13	6.946
File size	2 Mb			

Table 4. Channel resources allocation for hybrid lightweight security approach case study

Network elements	Channel idle (%)	Channel utilization (%)
Actuator	94.640	4.695
Server	96.030	6.080

**3.2. The 2<sup>nd</sup> case study without transport layer security**

The 2<sup>nd</sup> case study based the standard IoT heathcare environment without security approach to pass requests from the lower layer as IoT sensors to the network elements as actuator and then to the server to response into the incoming packets as imge file upload and acknwoldged with transmission control protocol (TCP) and user datagram protocol (UDP) connections. Table 5 and Table 6 showed the main evluation metrics to ths 2<sup>nd</sup> case study.

The proposed simulation system results indicate that the impact of security approch on performance across evaluation metrics the payload throughput is decreased due to the decreased number of packets, the delay is increased with the hybrid lightweight PRESENT, TEA security algrithms due to the verification and security features which work as filter and checkpoint to effects on network performance, in other words the proposed system increased computation process compared with state of without security due to the waiting time required for encryption process,so the proposed system focused on security with minimum resources requirements, as it showed in Figure 5 and Figure 6. Besides Table 7 showed the proposed system comparsion with other related works in this side.

Table 5. Payload throughput, avg delay, and packet loss rat of without security

Network element	Payload throughput/Kbps (Encapsulated/Decapsulated)		Avg Delay/ms	Packet loss rate (%)
	Frames/sec sent	Frames/sec received		
Actuator	73.736	72.967	16308.65	0.769
Server	65.671	62.605	18009.09	3.066
File size	2 Mb			

Table 6. Channel resources allocation for without security case study

Network elements	Channel idle (%)	Channel utilization (%)
Actuator	97.408	5.757
Server	98.853	8.455

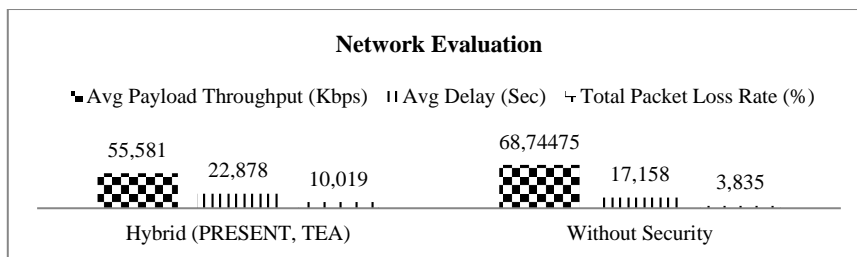


Figure 5. The average payload throughput, average delay, and packet loss rate

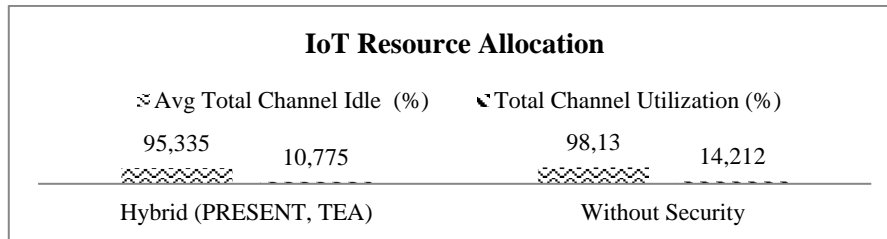


Figure 6. Channel resource allocation for the proposed system case studies

Table 7. The proposed system compared with other realted works

References	Algorithm	Throughput in Mb/ms	Time in ms
[27]	RC4+ECC+SHA-256	8	33
[28]	ECDSA+RC4+SHA-256	11	129
Proposed	PRESENT+TEA	31.7035	32.74

#### 4. CONCLUSION

The proposed algorithms PRESENT and TEA are used in this study to examine data security for IoT-based healthcare systems. This suggested integrated solution enhances the safe transfer of data from IoT devices to healthcare center personnel. The ECC authentication system and key generation technique are used to improve the key encryption and decryption process, preventing unwanted users from accessing the encrypted data. The suggested system's average payload throughput is 68.74475 Kbps, the average delay is 17.158 s, and the total packet loss rate is 3.835%, according to the used file upload image data. In future step, the proposed system stimulates the attack detection and prevention through identifying authorized users from unauthorized users.





#### REFERENCES

- [1] H. P. Alahari and S. B. Yalavarthi, "A survey on network routing protocols in internet of things (IoT)," *International Journal of Computer Applications*, vol. 160, no. 2, pp. 18–22, Feb. 2017.
- [2] "Internet of things securities," *UKEssays*, 2020. [Online]. Available: <https://www.ukessays.com/essays/information-systems/internet-of-things-securities.php>.
- [3] M. Tariq, T. Sato, G. Srivastava, V. Marojevic, and M. Goldenbaum, "IEEE access special section editorial: lightweight security and provenance for internet of health things," *IEEE Access*, vol. 9, pp. 67501–67503, 2021, doi: 10.1109/ACCESS.2021.3074326.
- [4] V. A. Thakor, M. A. Razaque, and M. R. A. Khandaker, "Lightweight cryptography for IoT: a state-of-the-art," *arXiv Prepr. arXiv2006.13813*, pp. 1–19, Jun. 2020, doi: 10.48550/arXiv.2006.13813.
- [5] A. Bogdanov *et al.*, "PRESENT: an ultra-lightweight block cipher," *International workshop on cryptographic hardware and embedded systems*, 2007, pp. 450–466, doi: 10.1007/978-3-540-74735-2\_31.
- [6] H. D. Azari and P. V. Joshi, "An efficient implementation of present cipher model with 80 bit and 128 bit key over FPGA based hardware architecture," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 14, pp. 1825–1832, 2018.
- [7] M. Sbeiti, M. Silbermann, A. Poschmann, and C. Paar, "Design space exploration of present implementations for FPGAS," *2009 5th Southern Conference on Programmable Logic (SPL)*, 2009, pp. 141–145, doi: 10.1109/SPL.2009.4914893.
- [8] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, Feb. 2019, doi: 10.3390/sym11020293.
- [9] S. Liu, O. V. Gavrylyako, and P. G. Bradford, "Implementing the TEA algorithm on sensors," *Proceedings of the 42<sup>nd</sup> annual Southeast regional conference*, Apr. 2004, pp. 64–69, doi: 10.1145/986537.986553.
- [10] B. Kim, J. Cho, B. Choi, J. Park, and H. Seo, "Compact implementations of HIGHT block cipher on IoT platforms," *Security and Communication Networks*, vol. 2019, Dec. 2019, doi: 10.1155/2019/5323578.
- [11] D. Hong *et al.*, "HIGHT: A new block cipher suitable for low-resource device," *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, Berlin, Heidelberg, vol. 4269, pp. 46–59, 2006, doi: 10.1007/11894063\_4.
- [12] B. J. Mohd, T. Hayajneh, Z. A. Khalaf, and K. M. A. Yousef, "Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation," *Security and Communication Networks*, vol. 9, no. 13, pp. 2200–2216, Mar. 2016, doi: 10.1002/sec.1479.
- [13] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," in *Cryptology ePrint Archive*, 2013.
- [14] S. Rana, Md. A. H. Wadud, A. Azgar, and M. A. Kashem, "A survey paper of lightweight block ciphers based on their different design architectures and performance metrics," *International Journal of Computer Engineering and Information Technology*, vol. 11, no. 6, pp. 119–129, Jun. 2019.
- [15] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: an overview of problems and proposed solutions," in *IEEE Security & Privacy*, vol. 3, no. 3, pp. 34–43, May–June 2005, doi: 10.1109/MSP.2005.78.
- [16] A. Poschmann, G. Leander, K. Schramm, and C. Paar, "New light-weight crypto algorithms for RFID," *2007 IEEE International Symposium on Circuits and Systems*, 2007, pp. 1843–1846, doi: 10.1109/ISCAS.2007.378273.





- [17] J. Patil, G. Bansod, and K. S. Kant, "Dot: A new ultra-lightweight sp network encryption design for resource-constrained environment," in *Proceedings of the 2<sup>nd</sup> International Conference on Data Engineering and Communication Technology*. Springer, vol. 828, pp. 249–257, 2019, doi: 10.1007/978-981-13-1610-4\_26.
- [18] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health information exchange," *Computers & Security*, vol. 67, pp. 73–88, Jun. 2017, doi: 10.1016/j.cose.2017.02.008.
- [19] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure medical architecture on the cloud using wireless sensor networks for emergency management," *2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications*, 2013, pp. 248-252, doi: 10.1109/BWCCA.2013.142.
- [20] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.
- [21] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, Feb. 2016, doi: 10.1016/j.future.2015.01.009.
- [22] A. Lakhan, A. H. Sodhro, A. Majumdar, P. Khuwuthyakorn, and O. Thinnukool, "A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks," *Sensors*, vol. 22, no. 6, p. 2379, Mar. 2022, doi: 10.3390/s22062379.
- [23] A. Alahdal and N. K. Deshmukh, "A systematic technical survey of lightweight cryptography on IoT environment," *International Journal of Scientific & Technology Research*, vol. 9, no. 3, 2020.
- [24] J. C. Hernandez and P. Isasi, "Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA," *Computational Intelligence*, vol. 20, no. 3, pp. 517-525, Jul 2014, doi: 10.1111/j.0824-7935.2004.00250.x.
- [25] M. Hassanaliyagh *et al.*, "Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: opportunities and challenges," *2015 IEEE International Conference on Services Computing*, 2015, pp. 285-292, doi: 10.1109/SCC.2015.47.
- [26] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7<sup>th</sup> International Conference on Body Area Networks*, 2012, pp. 269-275, doi: 10.4108/icst.bodynets.2012.250235.
- [27] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2033-2051, Feb. 2021, doi: 10.1007/s12652-020-02303-5.
- [28] S. S. Kumar and M. S. Koti, "An hybrid security framework using internet of things for healthcare system," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, pp. 1-10, 2021, doi: 10.1007/s13721-021-00329-z.

## BIOGRAPHIES OF AUTHORS







**Ameer Saad Kadhim**     an employee in the Directorate of Education in Babil Governorate master of Computer Science, participated in many local and international conferences. He is interested in IoT, IoHT, security algorithms, and advanced encryption methods. He can be contacted at email: ameer.saad@bab.epedu.gov.iq.



**Ali Haider Alazam**     an assistant lecturer at Al Mustaqbal Unevirsty College, Babylon, Iraq, master of computer science-Information security. He is intrested in information security, network architecture, encryption, cryptography, IoHT, and ECC. He can be contacted at email: ali.haider@mustaqbal-college.edu.iq.



**Noor Fahem Sahib**     is an assistant lecturer at Al Qasim Green University, Babylon, Iraq. She is interested in energy-specific sensors, security system, and networking, quality of service, TCP/IP-based security, public key cryptosystem, message authentication codes, and modern cryptography. She can be contacted at email: noor@fosci.uoqasim.edu.iq.