A SECURITY SERVICES OF PROPOSED SOCIAL WEB of THINGS

Ahmed H. MOHAMMED[1], Ali M. MAHDI[2]

The Social Network of Things (SWoT) is a technology that allows sharing of large amounts of information. There is a new challenge in protecting this information from exposure to risk during communication. This paper aims to provide a security framework for data collected through the health care system proposed as a case study of monitoring body temperature and heart rate that exceeds the threshold. The data is displayed directly on the patient's page on Twitter and sends a notification to the doctor's page and his family. From the security aspect, the system provided security services such as confidentiality using a proposed algorithm called Modified-PRESENT. In addition, integrity service using a hash for the encrypted data by (SHA3-512) and access control and authentication using (traditional login and Hash value matching). The system is secure. It uses social media to monitor the patient and make decisions for any authorized person (the doctor or his family), reducing the patient's burden and reducing the time in taking patient data in a secure, accurate, and fast way to maintain patient safety.

Keywords: IoT, SWoT, PRESENT, Modified-PRESENT, healthcare

1. Introduction

In recent years, Internet of Things (IoT) became an emerging discussion in research and practical implementations. IoT can be defined as a model that includes ordinary entities for sensing and communicating with the corresponding devices using internet [1] [2] [3]. WoT is also an expression to describe methods, software architectures, and programming shapes that provide natural objects, such as IoT, to be an integral part of the internet [4].WoT becomes a mechanism for discovering, controlling, monitoring, tracking, or communicating with physical objects through electronic devices connected with several network interfaces and eventually communicate with the broader internet [5] [6]. Also SWoT, a new concept, creates the interaction between people, services, and embedded devices person-to-device social interaction of physical objects by web communication at network levels will create different privacy issues and security, For SWoT to become a reality, there will be an urgent need for single application layer protocols with all physical smart devices and applications talking to each other, Regardless of how they are communicated in practice [7] [8] [9] [10].Social media

[1] PhD eng., Department of Computer Science, College of Education, Mustansiriyah University, Iraq

[2] Stud., Department of Computer Science, College of Education, Mustansiriyah University, Iraq, *Corresponding author’s Email: dr.ahmedh@uomustansiriyah.edu.iq

indicates the interactions amongst the people for the creation, sharing, and exchanging the information and the ideas such as Facebook, Instagram, Twitter, YouTube, Snapchat, and Vimeo accounts [11]. In general, the social network uses messages and websites to share all the content, including activities. Any object in a network will establish security issues and privacy weaknesses, these constraints will be hacked, these flaws and weak points can be manipulated in an environment with multi-billion devices [12]. In the Internet of Things, additional security features such as Confidentiality, Data Integrity or Authentication, non-repudiation, validation, and Availability are required [13][14].Thus, the term "lightweight" refers to a type of cryptographic cipher that has a tiny code size, low computing power, and low energy consumption. Because of these severe resource constraints, there is a rising demand for IoT-specific security solutions based on lightweight cryptography [15]. In SWoT, users can use standard protocols to access any device, the connection of various devices with SWoT simplifies integrating systems and applications and creates contrast but threatens confidentiality [16] [17]. The vital contribution to this paper is:

1- Design and implement a SWoT application for the healthcare system to manage the proposed security framework.

2- Proposed security framework provides security services such as (confidentiality, integrity, access control, authentication) for the SWoT application by using four steps:

Step 1: Confidentiality service is provided based on the proposed lightweight encryption algorithm (Modified-PRESENT algorithm) for sensors data (e.g., temperature, pulse) sent from Raspberry Pi to the Twitter app and the central server on the cloud.

Step 2: integrity service is provided based on a hash function for the encrypted data by (SHA3-512).

Step 3: access control service to the data sensors is provided using the web page by authentication according to the server (traditional login plus matching hash value).

Step 4: Monitoring all activities of users or doctors by the system administrator, such as logging in / out and a group of other tasks.

3- Maintaining patient information as a document in the central server database after applying security services.

4-The goal of sending data to the Twitter application (patient page) is that more than one doctor or user (his family) can monitor and make a decision as soon as possible.

2. Related Work

This section discusses some of the research papers on IoT security, as well as providing an overview of the security of healthcare systems.In (2013) Sufyan

S., etc., Study on Improving PRESENT Lightweight Algorithm. A new main-based S-box approach is introduced and extended to the PRESENT lightweight algorithm. The researchers did not apply the attacks to the proposed algorithm for measuring safety under the influence of time and memory [18].In (2017), Shatha H., in this thesis, suggests a new strategy called the Web of Thing Secure Socket Layer WoTSSL. An improved security channel communication between two servers (Raspberry Pi) uses encryption methods such as (algorithm, RSA, AES, TSFS) after collecting data from the sensors and storing it in the database. However, the researcher did not expose the proposed algorithm to attacks to measure security in time effect during transmission and did not address data security in SWoT [19].In (2019) Adil B., etc., Study on Secure Framework for Internet of Things Based e-Health System. The paper aims to the protection of Electronic Patient Records (EPR) in transit in e-health systems. The proposed security framework enables smart devices to encrypt data using lightweight and advanced algorithms [20].In (2019), Ahmed H.M, etc., in this paper, proposed an algorithm based on lightweight encryption called (LWAES). The goal is to achieve the fastest encryption and decryption time by deleting a stage (Mix Columns) from the design of (AES) [21]. In (2020) Chanapha Butpheng, Study on Privacy and Security on the Internet of Things-Cloud-Based e-Health Systems. In this paper, scientific studies from 2017 to 2020 were examined to know innovative technologies in Health and their development over time [22].

3. The Proposed SWoT System Design

The Web of Things uses intelligent interfaces to make a turn in the health field.The proposed health care security system's key task is to collect patient information using sensors to be displayed securely on the Twitter page. Health systems could be more vulnerable to threats than other Internet of Things applications.

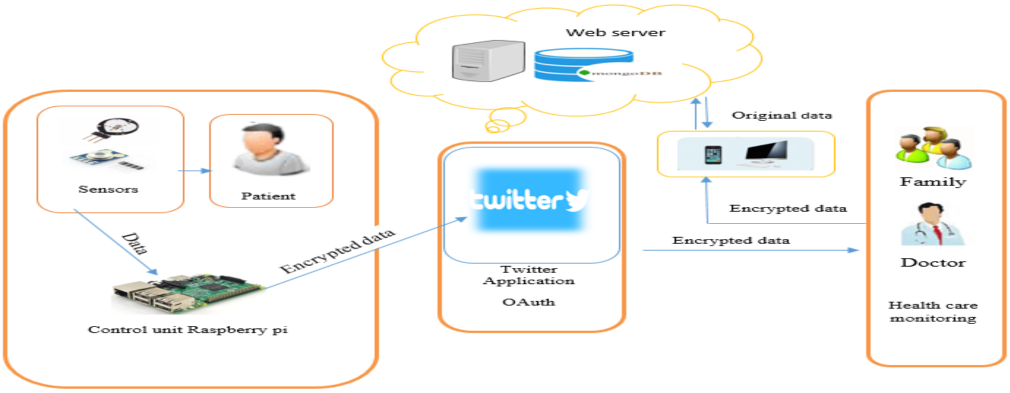

Fig 1 .The block diagram of the proposed security system architecture

In this proposed system, the essential system components consist of devices and objects used in the user home (the patient). For example, sensors (temperature, pulse) being the fundamental component of the system, as shown in Fig. 1. These sensors connect to the Raspberry Pi microcontroller where the patient's temperature and pulse are obtained. And the security services are applied to the sensors data that exceeds the given threshold limit (e.g. temperature is greater than 37, pulse is greater than 80) and displayed directly on the patient's personal Twitter page through the Open Standard of Authorization (OAuth) the same time a notification arrives on the page The doctor and individuals who follow the patient’s account on the Twitter page, and through a special browser, authorized persons can enter data and obtain data securely and store it in the patient’s database on the cloud. Thus ensuring that the system accesses the information quickly and safely as the proposed system passes through several stages discussed in detail**.**

3.1 The Proposed SWoT System Framework

This section will discuss the process of encrypting and decrypting using the proposed algorithm and calculating the hash value of the patient data. Fig. 2 illustrates the general architecture of the proposed system.

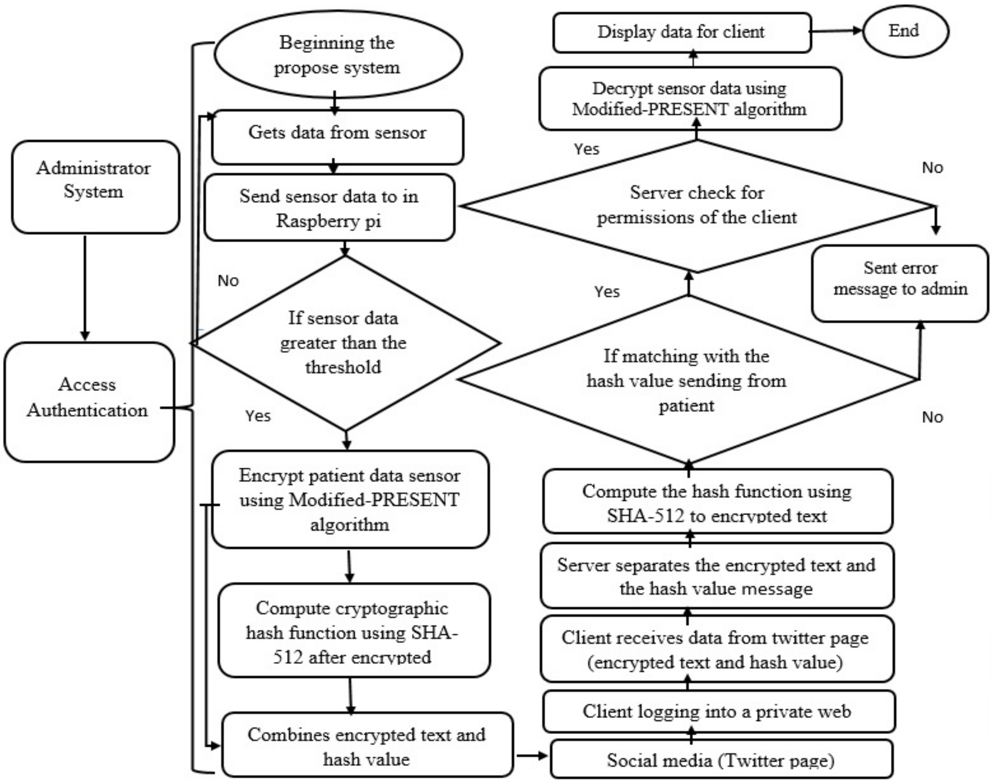
Beginning the propose system
Gets data from sensor
Send sensor data to in Raspberry pi
Administrator System
Access Authentication
No
If sensor data greater than the threshold
Yes
Encrypt patient data sensor using Modified-PRESENT algorithm
Compute cryptographic hash function using SHA-512 after encrypted
Combines encrypted text and hash value
Social media (Twitter page)
Client logging into a private web
Client receives data from twitter page (encrypted text and hash value)
Server separates the encrypted text and the hash value message
Compute the hash function using SHA-512 to encrypted text
If matching with the hash value sending from patient
Yes
No
Sent error message to admin
Server check for permissions of the client
Yes
No
Decrypt sensor data using Modified-PRESENT algorithm
Display data for client
End

Fig 2. Flowchart of the proposed SWoT system framework

A. Sensor Data Encryption

This phase discusses the process of encrypting the data and computing the hash value. The encryption process in the system encrypts the data (temperature and pulse) using Modified-PRESENT. Then, it is calculated the hash value for the data encrypted with (SHA-512). The encrypted text and the hash value are combined and sent as one block to the Twitter page. It will be executed Operation within Raspberry Pi.

B. Sensor Data Decryption

This side of the proposed system has been implemented in the server. The user will log into a private web browser using the traditional login (username and password) and fetch the encrypted text and hash value. From the patient page on Twitter, the server separates the encrypted text and the hash value, and display the procedure directly after calculating and matching the hash value and verify the user's permissions; it decrypts received data, then connect to the database to store the plaintext in the database (mongo).

3.2 The Proposed Modified-PRESENT

Secure information in these types of IoT applications is essential to choose a paradigm. The data will be ciphered, what algorithm can be used, and what the key will be shared. In this case, an asymmetric encryption approach is used. There a standard secret key is known by both the sender and the receiver. This type of encryption has the advantage of a short execution time, which allows for high-speed telematic applications using low computational power devices.

This section provides a detailed explanation of the proposed lightweight cryptographic algorithm. In this work, a new initialization vector (IV) to the plain text block was added to the present algorithm based on a random number (64 bits). IV was proposed to add more complexity and, at the same time, to preserve minimal computational cost. Therefore, the number of rounds has been reduced to increase the speed of the proposed algorithm without reducing the security of the PRESENT algorithm. In addition, the security of the Modified-PRESENT algorithm can be enhanced by using the shift state of the encryption process after a phase permutation p-layer and the s-box technique. Fig. 3. Shows the diagram of the Modified-PRESENT algorithm.

The Modified-PRESENT scheme's first aim is to improve the speed of the encryption/decryption algorithm. Thus, The Modified-PRESENT consists of IV: 64 bit, Block size: 64 bit, Key Length: 80 or 128 bit, Rounds: 16.

The proposed algorithm reduces encryption/decryption execution time compared to the original PRESENT algorithm and adding a new initialization vector (IV) to each plaintext block of the proposed algorithm makes it difficult for an attacker to predict this random value, which must be known in advance between the sender and receiver.

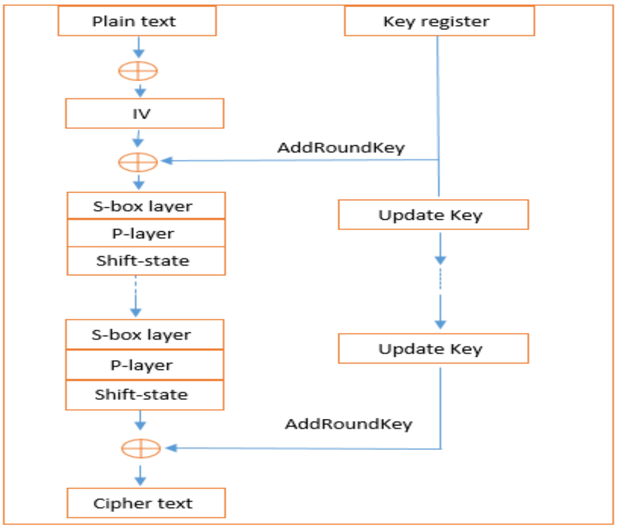

Fig 3. Diagram of the Modified-PRESENT algorithm

A. Encryption Process

Encryption is converting plain text into the encrypted text to secure data transmission over the network.

Firstly, the size of the input message is 64 bits. The XOR operation adds an initialization vector of the identical size to produce a new case, which is encrypted via XOR through the round key. Before sending the state's binary sequence into the permutation p-layer, the s-box technique was used to substitute it using a present s-box. The permutation table is used to process the p-layer, as shown in the PRESENT algorithm. The result was then processed by shifting it to the left based on the number of rounds of the key (for example, the first round, shift by one, and so on the rest of the rounds). In the entire process of the above actions, An 80-bit or 128-bit encryption key is manipulated by scheduling keys depending on the PRESENT algorithm [23] .There was a loop of 15 rounds until the last stage. The key [key16] is encrypted with the latest state for rounds through XOR to produce an encrypted text in the last operation.

B. Decryption Process

Decryption is converting the encrypted text into plain text by the recipient and applying an inverse process, such as inverse S-Box layer, P-layer.

Firstly, the key (key16) is generated and XORed with the ciphertext; then, the ciphertext state was decrypted via XOR through the round key. Before sending the state's binary sequence into the permutation inverse p-layer, the inverse s-box technique was substituted using a PRESENT inverse s-box. The permutation table is used to process the inverse p-layer based on the inverse permutation table, as shown in the PRESENT algorithm [23]. The result was then processed by shifting it to the right based on the key rounds. In the last procedure, the resulting state is XORed with the (IV) to produce plain text in the last procedure.

4. System Implementation

In the present scenario, two types of sensors are used. The first is the patient's temperature, and the second is the pulse sensor. Experiments are performed with a Raspberry Pi 3 board. After the sensors are read from the patient's side and matched with the threshold in the Raspberry Pi, the sensor data (temperature 38 and pulse 85) is encrypted. A hash value of the encrypted text is calculated and sent to the patient's Twitter page, displaying the encrypted text and the hash value as one block from the patient’s side on the Twitter page and sends a notification to the doctor's page and his family members who follow the patient's Twitter account. Then the main server page is accessed by only authorized users using private browser.

5. Security services of proposed SWoT Framework

All patient sensor data transmitted from raspberry pi to Twitter and to clients in the proposed healthcare system is secured in terms of data integrity, authenticity, and confidentiality. This section would include a thorough description of all of the security services offered by the proposed system.

5.1 Authentication / Access Control Security Services

The authentication and access control service provide two steps. The first step is to create a registry interface for all users in the system database, and the system administrator sets their permissions. The second step is the login process as well as server authentication, therefore, the client (doctor or authorized) must enter the email and password as well as the encrypted message block from the Twitter application (encrypted text and hash value) manually to process decrypt the data.

5.2 Confidentiality / Integrity Security Services

As indicated before, the patient's sensor reading data (heart rate and body temperature of people as input) is encrypted within the threshold before the raspberry pi sends the data to the client (Dr.) on the patient's Twitter page. The proposed lightweight encryption algorithm is used in the proposed healthcare system, which is a fast, efficient encryption method for protecting sensor data, which can achieve high throughput rates for high-speed communications.

The integrity portion of the patient sensor data sent from the program in raspberry pi to the clients is provided using SHA-512 also called as SHA-3 (Secure Hash Algorithm 3), which is the latest in the standard Safe Hashing Algorithm family. By calculating SHA-512 for the encrypted text and sending it as a single block to the patient's Twitter page, the client (Dr.) will calculate the

SHA-512 code for the provided encrypted text. If there is a match between the SHA-512 code for the sent message and the code for the computed message, the client (Dr.) can ensure that the data is completely intact and secure and has not been altered or tampered with during transmission.

This part of data integrity validation is also called data integrity. In the proposed system, the data integrity part is not concerned with the type of text encoding the message sent; which means that the SHA-512 hash code is generated for the encrypted output text, not for the original plain text. Fig. 4 shows sample data structure transmitted from raspberry pi to twitter that contains the integrity part (SHA3-512 hash code). After the client (Dr.) receives the data it connects to the server via a private browser. The server will match the generated hash through the ciphertext to the received hash; if they match, it will try to decrypt the received encrypted data and display its contents on a page (patient page). If there is a discrepancy between the received SHA-512 code and the hash code created, the customer (Dr.) will drop this received message and consider the data invalid.

6. Results

In this chapter, the proposed healthcare system is implemented using the proposed two-stage lightweight encrypting method. In the first stage, the execution time of the data read within the specified threshold is calculated from the sensors (for example, temperature 38, pulse 85) and a hash value of the ciphertext is calculated and sent to the Twitter page, where this part of the system is implemented using NodeJS language (v9.14.3) with the Express environment inside the Raspberry Pi.

The second stage is implemented after obtaining the ciphertext and the hash value as one block from the Twitter page by the authorized persons, which is executing between the client and the webserver on the cloud, which involves calculating the time of a ciphertext hash value, matching it, and then decrypting the sensor data. The proposed system has been evaluated from several aspects, as shown below.

6.1. Encryption/Decryption Time

The execution time was a critical parameter for evaluating any algorithm used in an IoT context. This algorithm must consume little time while providing a high level of protection. In this system, a comparison is made between the proposed encryption algorithm and the PRESENT encryption algorithm. We calculate the amount of time it takes to encrypt, and decrypt specific data read from the sensors. It is noticed that integrity data generation (SHA-512) takes considerable time if used, a comparison is made first with data integrity and then without data integrity as follows. Table 1. Shows the system execution time of both the PRESENT algorithm and Modified PRESENT algorithm with SHA-512 is calculated using a plaintext (76 byte) with Key (80 bits) and (128 bit) inside raspberry pi.

Table 1

Data Encryption Time in the PRESENT and Modified -PRESENT algorithm with SHA-512

Algorithm	Average Execution Time using key (80 bit) (without sha-512)	Average Execution Time using key (80 bit) (with sha-512)	Average Execution Time using key (128 bit)(without sha-512)	Average Execution Time using key (128 bit)(with sha-512)
PRESENT	0.5529 ms	0.9114 ms	1.2107 ms	1.7551 ms
Modified - PRESENT	0.0279 ms	0.1291 ms	0.1460 ms	0.9224 ms

6.2. NIST Test Suite Algorithms

There are many statistical tests for evaluating cryptographic algorithms' randomness properties [24]. NIST tests were used to compare the proposed algorithm's randomness to that of the PRESENT algorithm. This paper experimented with 100 bits obtained by executing the two algorithms on a text file for a set time. The results of statistical tests (15 NIST tests) the (P) value indicates that the random sequence ratio is based on the default value (0.01) for NIST tests. The results showed that the proposed algorithm passed all NIST statistical tests. Thus the binary sequence resulting from the proposed algorithm has a high level of randomness. Therefore, the proposed algorithm is suitable for the proposed system.

7. Conclusion

This study provides a security framework in health care that relies on popular social media applications (Twitter) to secure patient data. Moreover, display it safely on the patient's account on Twitter so that doctor or his family members can monitor the patient's condition continuously. The system provides several security services (confidentiality, authentication, and integrity). Confidentiality was provided through the Modified-PRESENT algorithm, which showed speed and complexity and passed NET tests. Thus, the system's application proved good, secure, and fast results in health care through interaction between users (doctors and patients) and taking advantage of SWoT. Therefore, we are planning to implement the full functionality of the system in other fields

REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660,Sep 2013.doi: 10.1016/j.future.2013.01.010
2. M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., vol. 38, pp. 8–27, 2018.doi: 10.1016/j.jisa.2017.11.002
3. R. Want and S. Dustdar, “Activating the Internet of Things [Guest editors’ introduction],” Computer (Long. Beach. Calif)., vol. 48, no. 9, pp. 16–20, 23 Sep 2015.doi: 10.1109/MC.2015.282

4. D. Zeng, S. Guo, and Z. Cheng, “The web of things: A survey,” J. Commun., vol. 6, no. 6, pp.424–438,1 Sep 2011.doi: 10.4304/jcm.6.6.424-438.
5. P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Internet of Things applications: A systematic review,”Comput.Networks,vol.148,pp.241–261,Jan 2019.
6. R. Khalaf, A. Mohammed, E. Essa, and H. Ali, “Controlling Smart Home Activities Using IoT,” ICCISTA 2019 - IEEE Int. Conf. Comput. Inf. Sci. Technol. their Appl. 2019, no. October, pp. 1–6, 2019.doi: 10.1109/ICCISTA.2019.8830664.
7. C. Cheng, C. Zhang, X. Qiu, and Y. Ji, “The Social Web of Things (SWoT)- Structuring an Integrated Social Network for Human, Things and Services,” J. Comput., vol. 9, no. 2, pp. 345–352,1 Feb 2014.doi: 10.4304/jcp.9.2.345-352.
8. M. G. Sarowar, M. S. Kamal, and N. Dey, “Internet of Things and Its Impacts in Computing Intelligence,” pp. 103–136, 2018.doi: 10.4018/978-1-5225-6207-8.ch005.
9. B. Cabral, C. Vasconcelos, and C. V. S. Prazeres, “The social web of things: Enabling the interaction of people and things on social networks,” Int. J. Web Based Communities, vol.10,no.4,pp.426–444,31 Oct 2014.doi: 10.1504/IJWBC.2014.065393.
10. V. Kanakaris, G. Lampropoulos, and K. Siakas, “A survey and a case-study regarding social media security and privacy on Greek future IT professionals,” Int. J. Hum. Cap. Inf. Technol. Prof., vol. 10, no. 1, pp. 22–37, Jan 2019.doi: 10.4018/IJHCITP.2019010102.
11. W. Akram and R. Kumar, “A Study on Positive and Negative Effects of Social Media on Society,” Int.J.Comput.Sci.Eng.,vol.5,no.10,pp.351–354,30 Oct 2017.
12. S. Rho and Y. Chen, “Social Internet of Things: Applications, architectures and protocols,” Futur. Gener. Comput. Syst., vol. 82,pp.667–668,May 2018.
13. W. Shafik and S. M. Matinkhah, “Privacy Issues in Social Web of Things,” 2019 5th Int. Conf. Web Res. ICWR 2019, pp. 208–214, Apr 2019.doi: 10.1109/ICWR.2019.8765254.
14. W. Li et al., “Security Analysis of the Lightweight Cryptosystem TWINE in the Internet of Things,” vol. 9, no. 1, pp. 793–810, 2015
15. M. Tausif, J. Ferzund, S. Jabbar, and R. Shahzadi, “Towards Designing Efficient Lightweight Ciphers for Internet of Things,” vol. 11, no. 8, pp. 4006–4024, 2017.
16. N. K. Singh and D. S. Tomar, “Privacy preservation of social media services: Graph prospective of social media,” Explor. Enterp. Serv. Bus Serv. Archit. Paradig., pp. 236–263, 2017.doi: 10.4018/978-1-5225-2157-0.ch016.
17. K. V. Rønn and S. O. Søe, “Is social media intelligence private? Privacy in public and the nature of social media intelligence,” Intell. Natl. Secur., vol. 34, no. 3, pp. 362–378, 16 Apr 2019.doi: 10.1080/02684527.2019.1553701.
18. S. S. M. Aldabbagh and I. F. T. Al Shaikhli, “Improving PRESENT lightweight algorithm,” Proc. - 2013 Int. Conf. Adv. Comput. Sci. Appl. Technol. ACSAT 2013, no. 1,pp.254–258,Dec 2013.doi: 10.1109/ACSAT.2013.57.
19. S. Habeeb, “Proposal to Develop Web of Things for Secure E-Health Service,” p. 130, 2018.
20. A. Bashir and A. H. Mir, “Secure framework for internet of things based e-health system,” Int. J. E-HealthMed.Commun.,vol.10, no. 4,pp.16–29,Oct 2019.
21. A. H. Mohammed and M. M. Jafer, “Secure web of things based on a lightweight Algorithm,” 1st Int. Sci. Conf. Comput. Appl. Sci. CAS 2019, no. September, pp. 216–221, 2019.doi: 10.1109/CAS47993.2019.9075831.
22. C. Butpheng, K. H. Yeh, and H. Xiong, “Security and privacy in IoT-cloud-based e-health systems-A comprehensive review,” Symmetry (Basel)., vol. 12, no. 7, pp. 1–35, 17 Jul 2020.
23. L. R. Knudsen, G. Leander, and A. Poschmann, “PRESENT : an ultra-lightweight block cipher PRESENT : An Ultra-Lightweight Block Cipher,” no. June 2014, 2007.
24. L. Hao and L. Min, “Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequences with application to image encryption,” Eur. Phys. J. Spec. Top., vol. 223, no. 8, pp. 1679–1697,Jun 2014.