International Journal of Engineering & Technology, *7 (4.25) (2018) 240-245*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Confidentiality and Integrity of Sensing Data Transmission in IoT Application

Rafide Hamad Khalaf[1*], Ahmed Hashim Mohammed[2]

[1,2] Al-Mustansiriyah University/Collage of Education/Computer Science Dept.
**Corresponding author E-mail: Aljumeily.rafidh@outlook.com*

Abstract

In the last few years the Internet of Things (IoT) has been developing new ways expected to connect billions of devices in different application of life. The increased numbers of connected devices are essentially smaller in size and low powered may be led to generate big data and face the security of data that transmitted. This paper proposed two types of security service for an IoT smart home application, the first security service is confidently which achieved by encrypting all data that sensor send to IoT server using AES-GCM or RSA-OAEP encryption algorithm moreover second security service is integrity all data that sensor send to IoT server which achieved using SHA3-512 encryption algorithm. In order to validate the security of sensor data results, we first had to implement the smart home application which consists of raspberry pi 3 and four sensors, the evaluation result shown a shorter average time 3ms when using AES-GCM algorithm whereas the RSA-OAEP algorithm had taken about 9ms, furthermore the integrity service had taken about 25% of encryption time.

Keywords: *Confidentiality, Integrity, Internet of things, Sensor Data, Encryption Algorithm*

1. Introduction

The term Internet of Things (IoT) was first coined by Kevin Ashton, the executive director of the Auto-ID Center as the title of a presentation he made at Procter & Gamble in 1999 [1]. IoT can be defined as a next-generation network of the Internet which is consists of communication of things, actuator, sensors, and other intelligent technologies that enables communication between person-to-object and object-to-object, Internet of things IoT [2]. IoT can as a dynamic global network structure with self-being and capable of standard and interoperability standard communication protocols where "physical and virtual objects" [3]. Due to rapid used the IoT techniques Leading to the rapid spread of applications of IoT techniques such as intelligent transportation and logistics, smart home/building, environmental monitoring, medical and healthcare, etc. [4] As well as rapid spread leads to its use in areas as diverse as healthcare (e.g. remote patient monitoring or monitoring of elderly people), smart grid, home automation (e.g. security, heating and lighting control) and smart cities (e.g. distributed pollution monitoring, smart lighting systems) [5]. Over time, and with rapid growth in manufacture of IoT devices such as (Sensors, Actuators, and Embedded system) some companies have submitted a study on the number of IoT devices that will be connected to the Internet and used in IoT network, As per Gartner company, 25 billion devices it is expected that, while Cisco expects 50 billion devices and Intel expects 28 billion devices and Data expects 80 billion devices will be connected to the Internet by 2020 [6].and with the proliferation of these devices in applications has led to a huge economic increase with a huge economic return, according to Accenture research report, the global industrial IoT market size in 2012 reached 20 billion US dollars, expected in 2020 will be more than 500 billion US dollars in recent years will have a high growth .

At the same time, based on the current level of input, by 2030, industrial Internet of things is expected to bring at least $10 trillion to the world economy[7]. But, with this huge number of applications and devices however, the smart home has become a major (mainstream) research and application interest in smart grid. Smart home refers to the use of ICT in home control, ranging from controlling appliances to automation of home features (windows, lighting, etc.)but, this devices that are connected to Internet networks may suffer from many problems one of the most important of these problems is security and privacy [8].

Security and privacy are widely acknowledged to represent critical issues and with the emergence of Low-power and Loss Networks (LLNs). They working group of companies to provide security solutions for IoT networks. and considered security and privacy issues in techniques related to physical systems, networks, software, and encryption [9].

However, IoT includes restricted devices in terms of resources (such as power and storage). Also, when applying heavy security alternatives to some nodes, such as a sensor and RFID tags, resources will be consumed and may turn the contract out of the implementation of key tasks. Since the contract can be battery-powered and expected to run for a long time, power consumption is critical in this network. Also, discuss security issues with respect to confidentiality, integrity, and availability, as well as Internet privacy issues [10].Therefore, we require specialized tools, techniques, and procedures for securing IoT networks and collecting, preserving and analyzing residual evidence of IoT environments [11].

The remainder of this paper is organized as follows. In the next section, we briefly related work. In the section3, we present the problem of IoT security and IoT security Services

In the section4, we briefly discuss Proposed Scheme of IoT Security Service. In Section 5, we provide the results and discussion of proposed system obtained in this paper. Finally in Section 6 conclude the paper.

2. Related work

In this section, we provide related research securing IoT objects and various authentication schemes to better manage communications between these objects.

In 2015, Bernard et al.[12] Worked on evaluating the OSCAR tool, a structure that provides end-to-end security in the Internet of things. It is based on the safety concept of the object that relates to security with the applied load. The structure includes authorization servers that provide customers with access secrets that enable them to request resources from a restricted CoAP contract. The contract is answered with the required signed and encrypted resources.

In 2016, Ko, Hajoon .[13] Provided a hybrid algorithm which has combined AES and ECC algorithms and has been applied in the security of IoT.

In 2016, Malina et al.[14] They provided a detailed assessment of the most important and most appropriate algorithms used on restricted devices that often appear in IoT networks. The performance of identical primitives was evaluate, such as ciphers block, hash functions, random number generators, and asymmetric primitives, such as digital signature schemes, privacy improvement schemes on various microcontrollers, smart cards, and mobile devices.

In 2017, Zhu,et al.[15] Presented a privacy-protection multi-server scheme, which is based on Chebyshev chaotic map operations. However, their scheme fails to protect privileged-insider attack, where a system insider of the RC acting as an attacker can guess user’s password using the stored information in the user’s device and registration request information during the registration phase by the attacker.

In (2017), Usman M., et al.[16] Proposed a lightweight encryption algorithm called Secure IoT (SIT) using a 64-bit block cipher by used 64-bit key to encrypt the data. Simulations result shows the algorithm provides substantial security in just five encryption rounds. The hardware implementation of the algorithm is done on a low-cost 8-bit micro-controller and the results of code size, memory use, and encryption/decryption execution cycles are compared with benchmark encryption algorithms.

In (2018), Parrilla L ., et al.[17] Proposed a compact system that enabling both the Elliptic Curve with Cryptography along to Advanced Encryption Standard (AES) algorithm with the requirements of a low area and support a set of switches. A co-processor designed to secure wireless sensor networks and communication protocols used. They have been proven that it consumes 15% less space, while better performance and 490% faster compared to crypto processors.

3. The IoT security services

The Security issues stem from the phenomenal pace of evolution in the internet network and the IT revolution today. As will The Internet network has become one of the main media outlets to connect between people with the introduction of technology in the world of the manufacture of smart things (sensors, actuators, and things). This rapid growth of hardware and services on the Internet has led to the proliferation of a large number of the unsafe node.

As well as, The Internet of things networks also contains a large number of heterogeneous devices. These devices require different communication technologies and protocols. And these devices suffer from several problems are (the device memory limited, processor limited, location, and very limited resources etc.) [18].

However, the report presented by Hewlett Packard on the state of security in the Internet of Things where it was concluded that 80 % of the tested devices had insufficient authentication and or authorization, 80 % showed privacy concerns, and 70 % used unencrypted communication channels [19].

Must be these devices should have the means to automatically protect their functioning and the data they contain. As well as the failure of the IoT hardware manufacturers to implement a strong security system on their products, as well as old versions of the equipment does not have any security measures at all. As well as Computer-controlled devices such as engines, breakers, locks, and information boards may be vulnerable to attackers who have access to the network. Because the Internet of things is a rich source of data will be vulnerable to sophisticated attacks[20].

In short, there are a number of security concerns that will be resolved mostly in the system Proposed. One of these solutions is to provide both (confidentiality, integrity, and authentication) for data transmission between server and client [21]. we look briefly at key security services in environments the internet of things.

3.1 Confidentiality

Confidentiality is one of the most important issues in network security. The Confidentiality on it is nature make each node is confidential in the data that you own and do not allow to share with neighbors or it has the ability to hide messages from a passive attacker so that any message is sent via the sensor network remains confidential. These may include smart meter measurements, billing, personal information, demographic data, and so forth [22].

3.2 Authentication

The Authentication process involves authentication of routing peers that involve in transferring data or the authentication for the source of data route. In fact, Authentication technology provides access control for IoT systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. Authentication allows integration of different IoT devices that are deployed in different contexts [23].

3.3 Authorization

The Authorization a process for granting consent to a system entity to access a system resource, or also as can be defined Authorization, method the access rights to different resources while Access Control mechanisms should guarantee access right of only authorized resources, or it ensures that users have the required control permissions to implement the operation they request to perform. In IoT system, Each and every IoT node may only support limited mechanisms for access verification which could be different from other connected objects to the same node. The data should be secured and accessible to authorized users only [24] [25].

3.4 Availability

The availability can be defined as the process of providing devices and data to users or only the authorized users whenever data and equipment are requested , As can be Definition of availability It ensures that the service is not interrupted in Internet objects, services are requested in real time, and the required services and data that are scheduled and submitted cannot be evaluated if not delivered in real time, The process determines whether the contract has the ability to use the resources and whether the network is available to communicate. Availability is also considered one of the most important security threats. The most important and most serious threat to availability is denial of service (DOS) attack [26].

3.5 Integrity

Data integrity, it ensures that messages sent between two parties have not been tampered with by a third party, or the process of preserving the data from any change throughout the lifespan, due to the flood of large data that is created by a large number of smart devices connected to Internet, Which reach up to Billions. So it is very difficult to make sure that the data collected and sent is not compromised. Encryption algorithms were used to ensure that the message was not tampered with by a third party and to ensure the integrity of the message such as (MD5, HASH, etc) [27].

4. Proposed scheme of IOT security service

Generally, Internet of thing systems applied widely in many areas of living such as smart home, smart building, and smart hotel etc. Smart home is one of the common application including various number of sensors for sensing an object and send its values to the server which required protection from malicious activities, The intruder may intercept, manipulate, and re-send one of these sensor data such temperature data value by inject his own fabricated data therefore, the large amount of data at risk which may lead to a defect in the entire network. The smart home is built with two types of sensors (DHT22, and ultrasonic sensor), the server monitors the traffic of temperature, or humidity data that has been sensed then send it to the right customers, each customer may specify specific conditions for notification of temperature, humidity, or traffic control readings.

Two different types of encryption algorithm (AES-GCM, RSA-OAEP,) were implemented beside SHA3-512 to provide security services (confidentiality and Integrity) for sensor data of smart home.

The sensor senses any change in the environment and send to the server. The (DHT22) sensor is extracting temperature or humidity after each 2sec, and the (ultrasonic senor) sensor sensing the motion after any event.

The server receives the data from temperature, humidity, and motion sensors via a specific GPIO (general-purpose input-output) port. When all the values (data) obtained from the sensors are read, where the server collects the data obtained from the sensors together into in packets format a single object (JSON).

4.1 Sensor data encryption-based AES-GCM / SHA3-512

When sensor data was collected as packet, the server encrypts these packets using AES-GCM encryption algorithm and secret key then to make integrity of data available the server calculates a hash function for that encrypted data using SHA3-512 as shown in the figure (1).

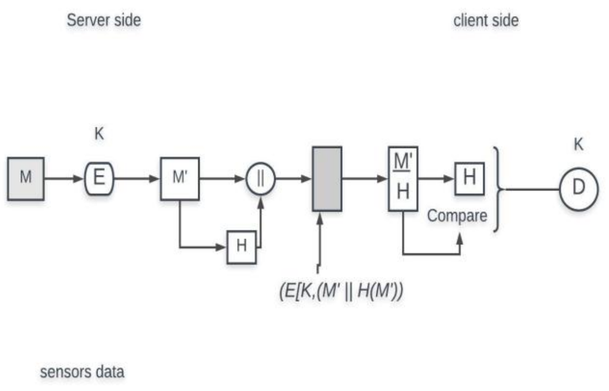

Fig.1: confidentiality, authentication and Integrity message

The encrypted data format is send via the web sockets protocol, this protocol sent the data in continuous manner after obtained from the server for all connected users according to their permissions, and display it to the visitor in client in an encrypted way across an HTML page as shown in the figure (2).

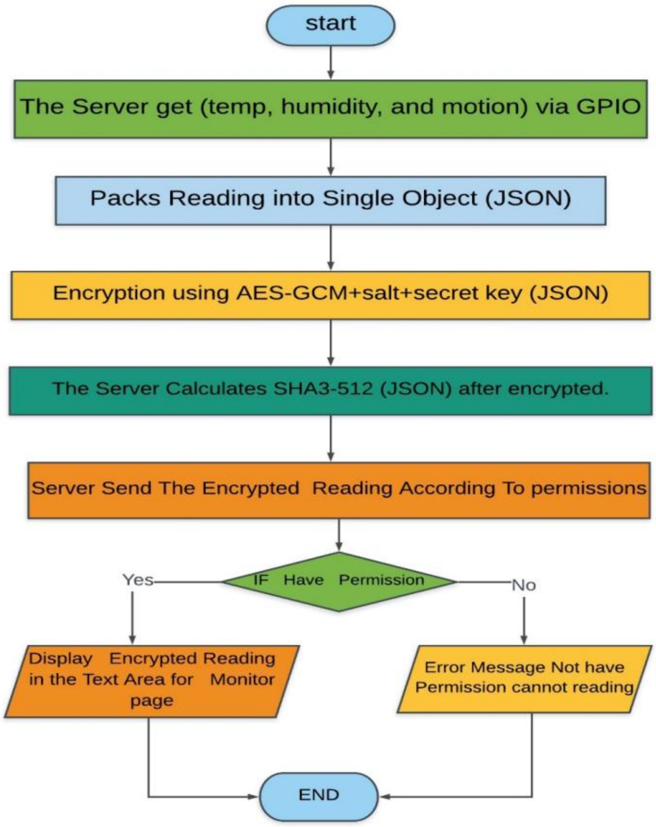
start
The Server get (temp, humidity, and motion) via GPIO
Packs Reading into Single Object (JSON)
Encryption using AES-GCM+salt+secret key (JSON)
The Server Calculates SHA3-512 (JSON) after encrypted.
Server Send The Encrypted Reading According To permissions
Yes
IF Have Permission
No
Display Encrypted Reading in the Text Area for Monitor page
Error Message Not have Permission cannot reading
END

Fig. 2:. Sensor Data Encryption based AES-GCM / SHA3-512

The steps of confidentiality and integrity based AES-GCM / SHA3-512 along with the sensor data transmission are shown in Algorithm 1.

```
Algorithm (1) :Sensor Data Encryption based AES-GCM/SHA3-512
Input: Get data from sensors
Output: Data encrypted
Step1: Server Gets Data from Sensor (Temp, humidity, motion)
  A: Get temperature & humidity by library bcm2835.
  B: Get Distance (motion in cm) by library (on/off).
Step2: Packs reading into a single object (temperature +humidity +motion + timestamp)
Step3: Encrypt value of Step2 using (AES-GCM+ Iv +Secret key)
Step4: calculates Hash value for Step2 by SHA3-512
Step5: Socket Emit to all connected users according to their permissions.
        If user has permission then
                Send the value of Step4
        Else
                Access Denied
        End if
Step6:End
```

4.2 Sensor data encryption-based RSA-OAEP / SHA3-512

RSA-OAEP is an asymmetric encryption algorithm has two keys (Public, private) that generated using key generation function. In this system the security of RSA-OAEP keys is increased by AES encryption. When sensor data was collected as packet, the server encrypts these packets using RSA-OAEP encryption algorithm and secret key as shown in the figure (3).

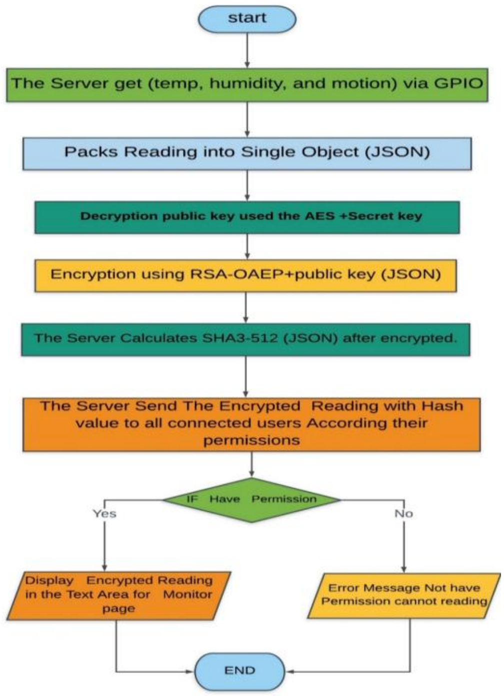
start
The Server get (temp, humidity, and motion) via GPIO
Packs Reading into Single Object (JSON)
Decryption public key used the AES +Secret key
Encryption using RSA-OAEP+public key (JSON)
The Server Calculates SHA3-512 (JSON) after encrypted.
The Server Send The Encrypted Reading with Hash value to all connected users According their permissions
IF Have Permission
Yes
No
Display Encrypted Reading in the Text Area for Monitor page
Error Message Not have Permission cannot reading
END

Fig. 3: Sensor Data Encryption based RSA-OAEP/ SHA3-512

Then to make integrity of data available the server calculates a hash function for that encrypted data using SHA3-512 as shown in the figure (4).

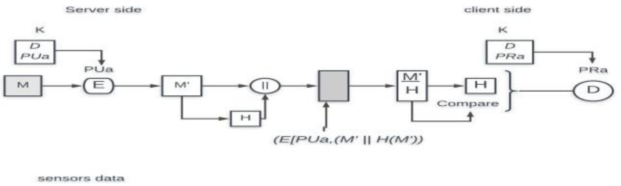

Fig. 4: confidentiality and integrity Message

The encrypted data format is send via the web sockets protocol and display it to the visitor in an encrypted way across an HTML page. The steps of confidentiality and integrity based RSA-OAEP/SHA3-512 along with the sensor data transmission is shown in Algorithm 2.

```
Algorithm (2) :Sensor Data Encryption Based RSA-OAEP/SHA3-512
Input: Data sensors
Output: Data encrypted
Step1: Generate public key and private key length of 2048 bits.
Step2: Store Key Pair as two separated strings (public, private)
Step3: Encrypted the value of S2 using AES algorithm using secret key.
Step4: Server Gets Data from Sensor (Temp, humidity, motion)
  A: Get temperature & humidity by library bcm2835.
  B: Get Distance (motion in cm) by library (on/off).
Step5: Packs reading into a single object (temperature +humidity +motion + timestamp)
Step6: Decryption public key by AES algorithm
Step7: Encrypt value of Step6 using RSA-OAEP and Public key
Step8: calculates Hash value for Step7 by SHA3-512
Step9: Socket Emit to all connected users according to their permissions.
        If user has permission then
                Send the value of Step9
        Else
                Access Denied
        End if
Step10:End
```

5. Result and discussion

In this section, client and server interaction model we used a cheap, small and powerful single board computer (Raspberry Pi3 model B+) running at 1.4GHz 64-bit quad-core processor, 1GB of RAM with Linux OS (Debian forked distribution called Raspbian).

The implementation of the AES-GCM algorithm is done with 64 bits key length, while in the RSA-OAEP algorithm the key length that we have used is 2048 bits. The measuring time for encryption and decryption of the data read from sensors calculating of the space complexity of which means increases In message size, with the increase in key length, using the system encrypting indicate how lightweight The algorithm is, and when it is less means that we have a lower amount of overhead. The proposed system was evaluated from several respects, as described below.

5.1 Encryption Time

The execution time is a very important parameter for the evaluation of any algorithm applying in IoT environment, furthermore the encryption and decryption time of a particular data read from sensors were evaluated for both AES-GCM and RSA-OAEP algorithm as follows:

5.1.1 Encryption Sensor Data Based AES-GCM

The average encryption time for encrypt 87 bytes of message size without AES-GCM and with AES-GCM algorithm was listed in table(1) among different number of users, as a result the server time was taken to encrypt a fixed message size affected by the number of the connected users.

TABLE 1: Data Encryption Time using AES-GCM

Type	Message size in bytes	key Length	Number of users	Average Encryption Time (without sha3-512)	Average Encryption Time (with sha3-512)
AES-GCM	87 Bytes	64 bits	1 user	3 ms	4 ms
	87 Bytes	64 bits	2user	4 ms	5 ms
	87 Bytes	64 bits	4user	5 ms	6.5 ms
	87 Bytes	64 bits	6user	7 ms	9 ms
	87 Bytes	64 bits	8 user	10 ms	12 ms
	87 Bytes	64 bits	10 user	12 ms	15 ms

Another evaluation of average encryption time of using AES-GCM algorithm is listed in table 2 among different number of (1-10) users along with temperature and humidity data sensors, it's was indicated that the server time taken to encrypt a fixed message size affected by the number of the connected users.

TABLE 2: Data Encryption Time with Different Message Size and Number Of Users

Type	Message size	Key Length	Number of users	Average Encryption Time in milliseconds
AES-GCM	71 bytes	64 bits	1 user	2 ms
	71 bytes	64 bits	2 user	3 ms
	71 bytes	64 bits	4 user	5 ms
	71 bytes	64 bits	8 user	6 ms
	71 bytes	64 bits	10 user	8 ms

5.1.2. Encrypting Sensor Data based RSA-OAEP

By using the RSA-OAEP algorithm 2084 bits of key Length, the time consumed by the server was longer than with AES-GCM besides the server time taken to encrypt the message size is also affected by the number of the connected clients as shown in **TABLE** (3).

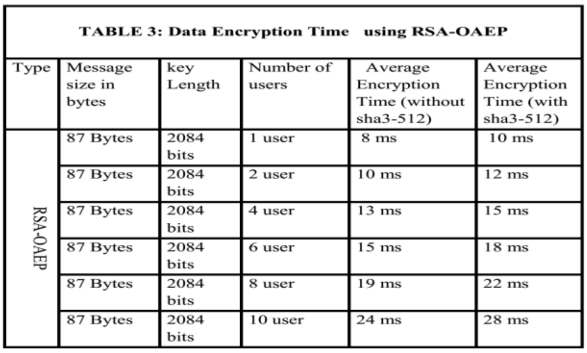

TABLE 3: Data Encryption Time using RSA-OAEP

Type	Message size in bytes	key Length	Number of users	Average Encryption Time (without sha3-512)	Average Encryption Time (with sha3-512)
RSA-OAEP	87 Bytes	2084 bits	1 user	8 ms	10 ms
	87 Bytes	2084 bits	2 user	10 ms	12 ms
	87 Bytes	2084 bits	4 user	13 ms	15 ms
	87 Bytes	2084 bits	6 user	15 ms	18 ms
	87 Bytes	2084 bits	8 user	19 ms	22 ms
	87 Bytes	2084 bits	10 user	24 ms	28 ms

Another evaluation of average encryption time of using RSA-OAEP algorithm is listed in table (4) among different number of (1-10) users along with temperature and humidity data sensors.

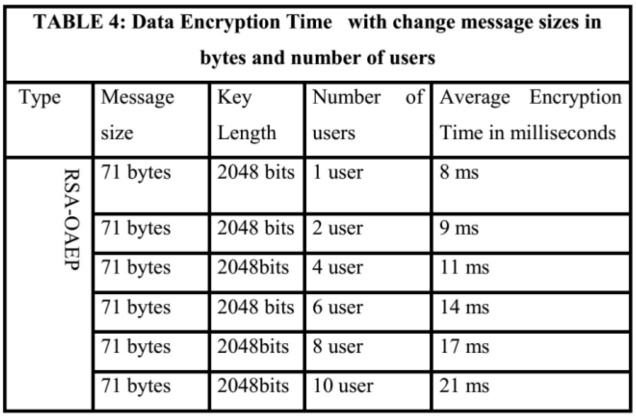

TABLE 4: Data Encryption Time with change message sizes in bytes and number of users

Type	Message size	Key Length	Number of users	Average Encryption Time in milliseconds
RSA-OAEP	71 bytes	2048 bits	1 user	8 ms
	71 bytes	2048 bits	2 user	9 ms
	71 bytes	2048bits	4 user	11 ms
	71 bytes	2048 bits	6 user	14 ms
	71 bytes	2048bits	8 user	17 ms
	71 bytes	2048bits	10 user	21 ms

5.2 Memory Consumption

Memory usage is a major concern in resource constraints of IoT devices, so it's essential to use cryptographic algorithms not require too large memory to be suitable for posting in IoT environment, furthermore the encryption and decryption memory consumption of a particular data read from sensors were evaluated for both AES-GCM and RSA-OAEP encryption algorithms.

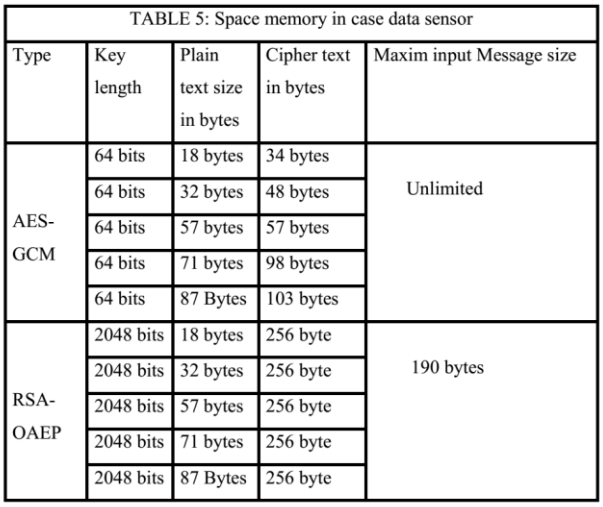

TABLE 5: Space memory in case data sensor

Type	Key length	Plain text size in bytes	Cipher text in bytes	Maxim input Message size
AES-GCM	64 bits	18 bytes	34 bytes	Unlimited
	64 bits	32 bytes	48 bytes	
	64 bits	57 bytes	57 bytes	
	64 bits	71 bytes	98 bytes	
	64 bits	87 Bytes	103 bytes	
RSA-OAEP	2048 bits	18 bytes	256 byte	190 bytes
	2048 bits	32 bytes	256 byte	
	2048 bits	57 bytes	256 byte	
	2048 bits	71 bytes	256 byte	
	2048 bits	87 Bytes	256 byte	

As can be shown from the above table (5), AES-GCM encryption algorithm is more adaptive than RSA-OAEP encryption algorithm because its cipher text size is changing according to the plain text size while RSA-OAEP encryption algorithm while the RSA-OAEP output cipher text is fixed at 256 bytes long, the input message is also limited in this algorithm to only 190 bytes making it unusable with larger data encryption processes.

6. Conclusion

In the near future Internet of Things will be an essential element of our daily lives, numerous energy constrained devices and sensors will continuously be communicating with each other the security of which must not be compromised.

In the proposed system we implement the (AES-GCM, and RSA-OAEP) encryption algorithm and calculate the amount of time have taken to encode and decode) accordingly the implementation have shown the AES-GCM algorithm a suitable to be adopted in IoT applications because it was consumed minimal time and offer considerable security also It is noticed that integrity data generation using SHA3-512 takes considerable time.

References

[1] I. C. L. Ng and S. Y. L. Wakenshaw, "The Internet-of-Things: Review and research directions," *Int. J. Res. Mark.*, vol. 34, no. 1, pp. 3–21, 2017.

[2] H. Javdani and H. Kashanian, "Internet of things in medical applications with a service-oriented and security approach: a survey," *Health Technol. (Berl).*, vol. 8, no. 1–2, pp. 39–50, 2018.

[3] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Networks*, vol. 129, pp. 444–458, 2017.

[4] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, 2017.

[5] L. Chen, "Security Management for The Internet of Things," *ProQuest Diss. Publ.*, 2017.

[6] S. Deng, "Industrial IoT Technologies and Applications," vol. 202, pp. 102–110, 2017.

[7] K. Bu, M. Weng, Y. Zheng, B. Xiao, and X. Liu, "You Can Clone but You Cannot Hide: A Survey of Clone Prevention and Detection for RFID," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1682–1700, 2017.

[8] Z. Kamal, A. Mohammed, E. Sayed, and A. Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies," *WSN World Sci. News*, vol. 67, no. 672, pp. 126–148, 2017.

[9] S. El Jaouhari, A. Bouabdallah, and J. M. Bonnin, *Security Issues of the Web of Things*, 1st ed. Elsevier Inc., 2017.

[10] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018.

[11] A. Gantait, J. Patra, and A. Mukherjee, “Design and build secure IoT solutions , Part 1 : Securing IoT devices and gateways,” *IBM Dev.*, no. May, pp. 1–20, 2016.

[12] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, “OSCAR: Object security architecture for the Internet of Things,” *Ad Hoc Networks*, vol. 32, no. January, pp. 3–16, 2015.

[13] H. Ko, J. Jin, and S. L. Keoh, “Secure Service Virtualization in IoT by Dynamic Service Dependency Verification,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1006–1014, 2016.

[14] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, “On perspective of security and privacy-preserving solutions in the internet of things,” *Comput. Networks*, vol. 102, pp. 83–95, 2016.

[15] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, “Survey of Security Advances in Smart Grid: A Data Driven Approach,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[16] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,” vol. 8, no. 1, pp. 1–10, 2017.

[17] L. Parrilla, E. Castillo, J. A. López-Ramos, J. A. Álvarez-Bermejo, A. García, and D. P. Morales, “Unified compact ECC-AES co-processor with group-key support for IoT devices in wireless sensor networks,” *Sensors (Switzerland)*, vol. 18, no. 1, pp. 1–22, 2018.

[18] P. Fremantle and P. Scott, “A survey of secure middleware for the Internet of Things,” *PeerJ Comput. Sci.*, vol. 3, p. e114, 2017.

[19] P. Siano, G. Graditi, M. Atrigna, and A. Piccolo, “Designing and testing decision support and energy management systems for smart homes,” *J. Ambient Intell. Humaniz. Comput.*, vol. 4, no. 6, pp. 651–661, 2013.

[20] J. M. Batalla, A. Vasilakos, and M. Gajewski, “Secure Smart Homes: Opportunities and Challenges,” *ACM Comput. Surv.*, vol. 50, no. 5, pp. 1–75, 2017.

[21] A. Rayes and S. Salam, “Internet of things-from hype to reality: The road to digitization,” *Internet Things From Hype to Real. Road to Digit.*, no. November, pp. 1–328, 2016.

[22] Y. Challal, E. Natalizio, S. Sen, and A. M. Vegni, “Internet of Things security and privacy: Design methods and optimization,” *Ad Hoc Networks*, vol. 32, pp. 1–2, 2015.

[23] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” *J. Netw. Comput. Appl.*, vol. 84, no. January, pp. 25–37, 2017.

[24] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018.

[25] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[26] D. G. Padmavathi and M. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 1, pp. 1–9, 2009.

[27] S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, “A security-and quality-aware system architecture for Internet of Things,” *Inf. Syst. Front.*, vol. 18, no. 4, pp. 665–677, 2016.