Improvement of the Secure Integration of IoT and Cloud Computing using Hybrid Encryption

P. DR. NADEEM CHAHIN [1], Eng. ABEER MANSOUR [2]
Electronics and Communication Engineering [1, 2]
Damascus University [1, 2]
DAMASCUS, SYRIA

Abstract: Wireless Sensor Network (WSN) is an essential technology in many Internet of Things (IoT) applications, and since sensor nodes suffer from limited resources, it has become possible to overcome storage capacity problems using cloud computing, the integration of Internet of Things (IoT) with cloud computing (CC) seeks to achieve new levels of efficiency in service delivery. Security and privacy are key factors that slow down the rapid and widespread adoption and deployment of both IoT and cloud computing. In the proposed model, an integrated IoT system with cloud computing was developed starting from the analysis, and design, to the implementation to connect IoT devices with the cloud, the security is achieved by using a hybrid encryption mechanism which provides the performance advantages of symmetric and asymmetric encryption algorithms. Where the Elliptic Curve Cryptography (ECC) algorithm is used for key generation and AES (Advanced Encryption Standard) algorithm is used for encryption and decryption of the sensors' data to provide a reliable computing environment. We have implemented the proposed system and showed the results of using CONTIKI COOJA 3.0 that connected with the cloud service provider, Evaluate a set of performance metrics such as power consumption, packet delivery ratio, and the algorithm execution time, in addition to verifying network immunity against the black hole attack.

Key Words: Internet of Things, Cloud Computing, Security, Hybrid Encryption, Reliability.

Received: October 22, 2022. Revised: November 15, 2022. Accepted: November 30, 2022. Published: December 8, 2022.

1 Introduction

From their emergence, the two concepts of the Internet of Things (IoT) and cloud computing (CC) have evolved separately. For many years, they have seen independent evolution in their hardware and software aspects. In its evolution, IoT faces many problems among them storage capacity, energy efficiency, and computational capabilities. While looking for solutions to these problems, scientists found that CC could help to solve them. In addition, the Internet of Things could allow CC to handle real-world objects in a more dynamic way to deliver new attractive services and applications in some practical applications.

Hence, the need to merge the Cloud and IoT technologies emerge. As a result, the concept of the Cloud of Things (CoT) was born. This integration is useful because the resulting system is more powerful, and intelligent and offers promising solutions to the users. However, CoT faces a large number of challenges such as security, privacy, reliability, scalability, heterogeneity, power consumption, standardization, and others [1].

Security and privacy are frequently discussed when talking about IoT and cloud computing integration. since the cloud consists of a large number of servers that host applications responsible for carrying out computer processing operations on data collected from IoT devices[2], the network will be vulnerable to many attacks such as MIM (Man in the Middle), Sinkhole attack, Vampire Attack, Jamming Attack. One of the most important attacks that limited resources networks suffer from is the blackhole attack, in which the attacking node drops all packets sent to another node in its root, and aims to steal the important information or waste the network resources [3]. To protect the data that is exchanged in the network and stored in the cloud, encryption technologies (like lightweight cryptographic algorithms) are used, which help to securely transmit data over the wireless medium and provide

reliability, confidentiality, data integrity, and non-repudiation [4].

Within the framework of security and privacy requirements, and to deal with the challenges of IoT devices, a lightweight encryption solution based on a hybrid encryption system is used to provide better protection for data stored on the cloud. hybrid encryption is a combination of symmetric and asymmetric encryption algorithms to provide more security for the data before it is stored on the cloud.

The remaining part of this paper is organized as follows. Section 2 provides the related works on the integration between the internet of things and cloud computing. Section 3 provides the research materials and methods. Section 4 shows the performance results with detailed descriptions. Section 5 concludes the paper.

2 Related Works

The integration between the wireless sensor networks and cloud computing can be achieved by creating virtual backups of sensors and their information on the cloud and the same calculations are performed on physical and virtual sensors [7] through a simple model of the principle of Distributed Shared Memory (DSM).

A different approach in [8] discusses a novel three-level architecture that integrates WSN, IoT, and cloud computing capabilities. At the bottom, the SPL (Sensor Processing Level) clusters all sensors. The DAL (Data Analysis Level) is considered a local interface between sensors, the cloud platform, and the users or health specialists. The DAL server backend consists of local algorithms for data aggregation and event-triggered alarms. The graphic user interface available at this level allows real-time monitoring of data gathered from sensors. The CPL (Cloud Prediction Level), allows data storage, data correlation, and prediction. It generates useful information for users and specialists. Using this layer, the health specialist can provide an anticipative reaction to health issues considering also the air quality level. The paper provides an implementation solution for advanced AAL (Ambient Assisted Living) application implementation. The novelty is not only in the different processing levels but also in the implementation that provides solutions for ensuring a fast reaction speed in case of emergency, together with access to complex prediction algorithms.

The research in [9] proposed a general architecture called (IoTaaS) to represent and guide the integration process. This architecture supports security by providing a secure gateway that connects the IoT system to the cloud, supporting data encryption for data passed from/to the cloud. Providing the authentication manager to ensure only authorized parties have access to the IoT system and cloud services. Delegating all database operations to the data manager and handler to ensure only valid operations are carried out. The architecture also supports real-time interactions by providing the real-time interactive handler, which uses artificial intelligence and context awareness to provide real-time access to IoT systems. Real-time interaction is also supported by making modifications to the data management system and using context information to reduce response time.

IoT devices are mostly powered by batteries and have a limited amount of memory and processing capacity. Designing a security mechanism that can suit these small devices is a challenging task, and there are concerns about cloud administrators who can access the collected data. and to protect this data, various technologies such as encryption have been proposed [2].

We can classify the encryption algorithms into two general categories: the Symmetric Encryption Algorithm (Private-Key) and the Asymmetric Encryption Algorithm (Public-Key) [4] shown in Fig.1. The symmetric key technology uses a single key called the secret key that uses less mathematics, and less calculation, on the other hand, the asymmetric key technology uses both public and private keys, leads to more processing and consumes more power but the keys are more strong and secure[6].

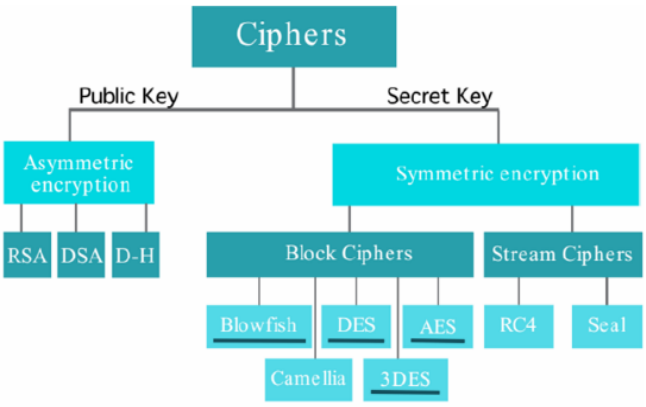

Fig.1 Classification of cryptographic algorithms [6]

The results of LabVIEW 2016 simulations to study several encryption algorithms in [10] showed that AES is the best encryption algorithm in terms of speed, productivity, and low power consumption because in the 128-bit key encryption it can encrypt a 128-bit block (the largest encryption block for encryption algorithms) in just 14 cycles. The DES (Data Encryption Standard) algorithm then comes in second place as the best performance, while 3DES

(Triple DES) and RC2 have the same level of performance, RSA (Rivest–Shamir–Adleman) has the lowest level of performance in terms of speed and productivity.

In the research [11] a hybrid encryption system is proposed using different encryption algorithms to provide the advantages of both symmetric and asymmetric encryption using ECDH (Elliptic-curve Diffie–Hellman) to generate keys and perform a digital signature to achieve authentication, and AES is used for encrypting the data.

The researchers in [13] proposed a hybrid encryption approach combining the ECC algorithm and the ElGamal algorithm. The encrypted information is uploaded to the cloud for storage, in different channels and passwords. The user who authenticates the strategies can download the encrypted data and decrypt them by a synchronous key that uses the ECC-ElGamal algorithm. The simulation was performed using MATLAB 2014a and calculating various performance factors such as execution time, packet delivery rate, and delay, and comparing these results with the traditional methods and found that it offers 12%, 31%, and 8% in terms of packet delivery rate, delay and execution time in respect.

3 Research materials and methods

The work was performed using a computer with a core i5 processor (2.20 GHz) – 8 GB RAM Windows 10 operating system (64 Byte). virtual tool (VMware virtual machine) was used to run Ubuntu (64 Byte and 8 GB RAM) and the simulation was performed on CONTIKI COOJA 3.0 which supports the Internet of Things networks and all protocols in the field of networks. It is considered an emulator and not a simulator because its performance is closer to reality and it performs a real operation on the sensors devices in the network. The work has been done on Skymote nodes type, the simulation language used is C.

In the proposed model, the network was implemented according to the following steps, fig.2:

1. Choose the gateway node that connects the nodes to the Internet.
2. Discover the nodes by the sink node.
3. Generate keys by sink node using the ECC algorithm and distribute them to nodes in the network.
4. Encrypt the sensor data using the AES algorithm at the nodes.
5. Transfer the encrypted data from nodes to the cloud server.
6. Study a set of metrics such as power consumption, execution time, and packet delivery ratio, and compare the results with a reference model and with other studies.
7. Apply and detect a blackhole attack on the network to verify the immunity of the network and the effectiveness of the proposed mechanism.

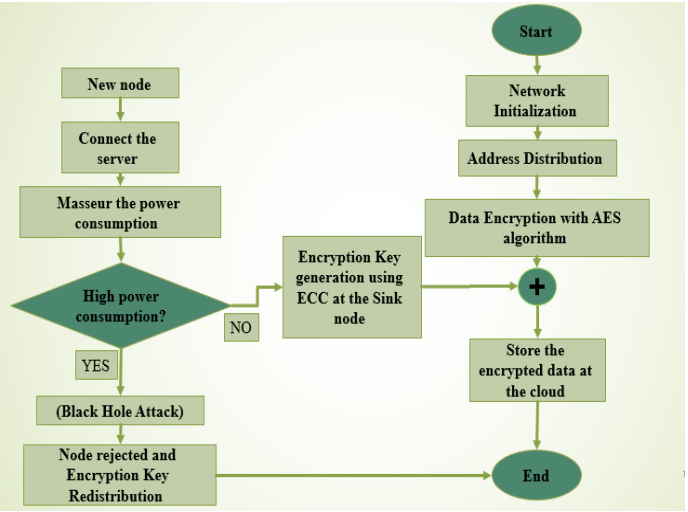

Fig.2 Flowchart of the proposed model

The proposed model was achieved in three scenarios on an increasing number of nodes (10-15-20 nodes in order) with a network area (100*100 m^2):

- Scenario I (no encryption): a study of the Internet of Things system connected to the cloud server without applying any encryption algorithms.
- Scenario II (encryption): apply the proposed hybrid encryption algorithm on the same network in the first scenario and compare the results for both packet delivery ratio, power consumption, and execution time.
- Scenario III (blackhole attack): Apply the blackhole attack on the network and detect the attack while explaining the usefulness of the proposed method of protection.

The COOJA is connected to a cloud using smarterasp.net which gives the possibility of building a private cloud from the beginning, downloading and modifying algorithms as needed, fig.3.

Fig.3 Cloud Service Program Interface

The data collected from the sensors is sent in encrypted form to the cloud server for storage, the decryption can be performed only by users authorized to enter and had the decryption ECC code of the network which ensures confidentiality and reliability.

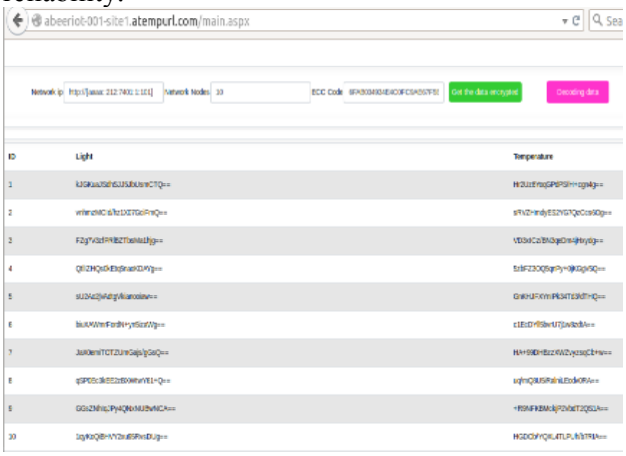

Fig.4 Displaying encrypted sensors data on the cloud site

View sensors data after decryption using a special decryption code:

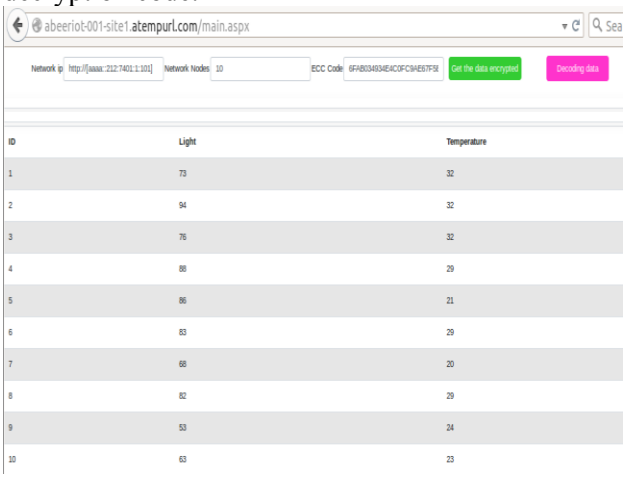

Fig.5 Display the sensor data after decoding on the cloud site.

4 Results and comparison

The performance of the proposed model was tested, analyzed, and compared with the reference state and then the results were compared with existing studies.

4-1 Packet Delivery Ratio (PDR %):

PDR (Packet Delivery Ratio) refers to the ratio of the total number of packets received at the destination to the total number of packets created during the simulation, expressed according to the equation [5]:

$$PDR = \frac{\sum_{i\varepsilon S} npacketsReceived(i.d)}{\sum_{i\varepsilon S} npacketsSent(i.s)}$$

Where S is a set of sessions created during the simulation and npacketsReceived (i.d) and npacketsSent (i.s) are the number of packets received at the destination d and sent from source s for session i, respectively.

We note that for the first and second scenarios there is no loss of packets where the delivery ratio is 100%. The proposed algorithm did not cause any loss of packets in the network. At the attack scenario, we can find that the attacking node causes a significant loss of packets, in fig.6.

The attack can be detected by monitoring the number of received packets because the noticeable increase in the total number of messages exchanged in the network nodes is due to the increase in the number of control messages sent by the victim nodes trying to rejoin the network, shown in fig.7.

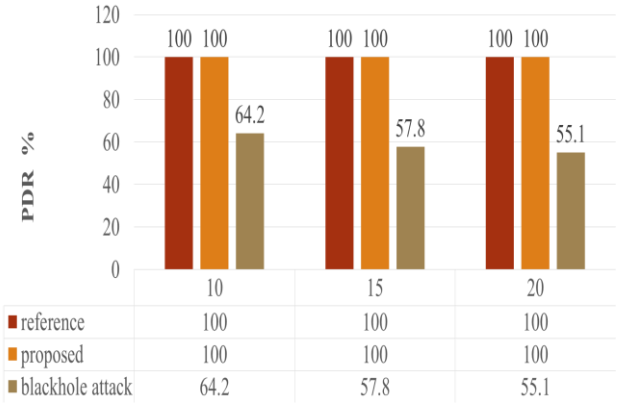

Fig.6 Packet Delivery Ratio%

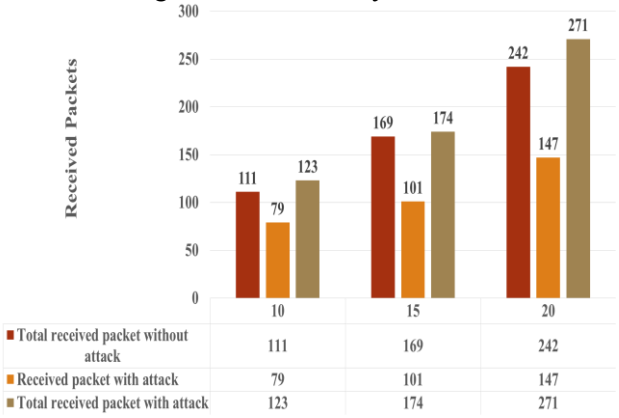

Fig.7 Number of total packets in case of attack

4-2 Power Consumption:

The simulation gives a set of values related to power consumption by each node individually and in detail (CPU power, LPM power, Listen power, Transmit power) and the result of power consumption for each node, which is the sum of all previous values. Expressed according to the equation [14]:

$$power\ (mW) = \frac{Energest_{value} \times current \times voltage}{RTIMER\_SECOND \times Runtime}$$

$Energest_{value}$, Current, and Voltage are taken from the simulator and RTIMER_SECOND is a Clock.

The small increase in the power consumed due to the encryption process is acceptable compared to other studies and does not affect the functioning of the network.

When applying the blackhole attack, a significant increase in power consumption can be observed, and the increase is caused by the desire of the victim nodes to rejoin the network and send more control messages, Fig.8.

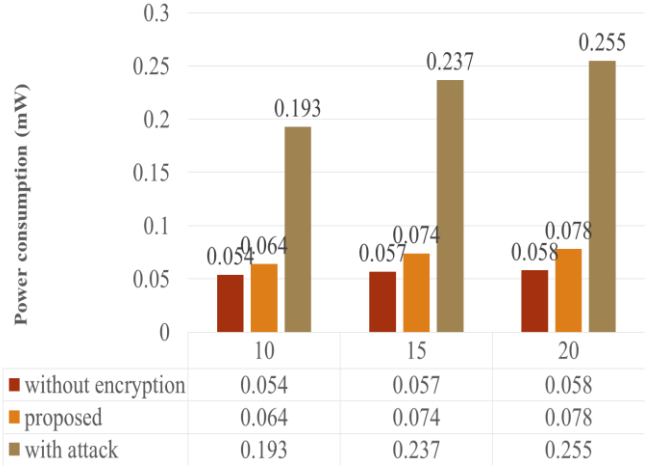

Fig.8 Power Consumption (mW)

4-3 Execution time of the algorithm:

The Execution time of the algorithm was obtained by using a computer Core i5 processor (7th generation) and (8RAM) and SSD hard because the results in the encryption speed change depending on the state of the device, all values measured by ms, the keys are distributed after detection of all the surrounding nodes, with a maximum simulation runtime (2.7 m) for the 10-node scenario. Fig.9 shows in detail the time required for the process of key generation, encryption, and decryption, and the total execution time of the algorithm.

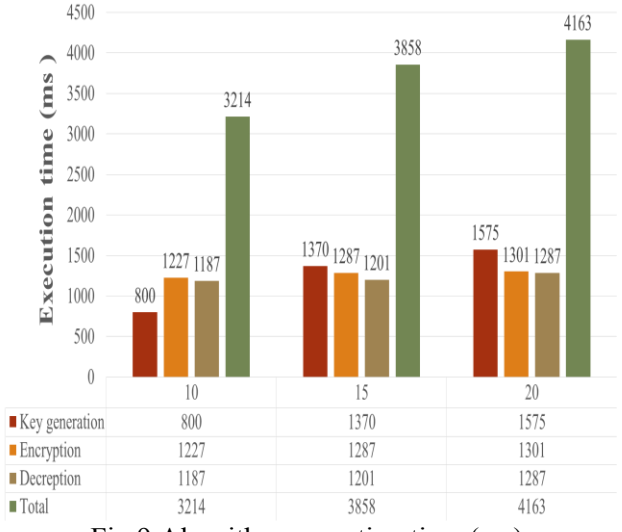

Fig.9 Algorithm execution time (ms)

4-4 compare the results of the proposed model with existing studies:

- Compare power consumption:

The researchers proposed a hybrid encryption model in [14] using the AES algorithm to encrypt data with ECDH to generate keys and authentication, and we note that the proposed model offers suitable and better solutions for energy consumption as the data exchange rate increases in the network,fig.10.

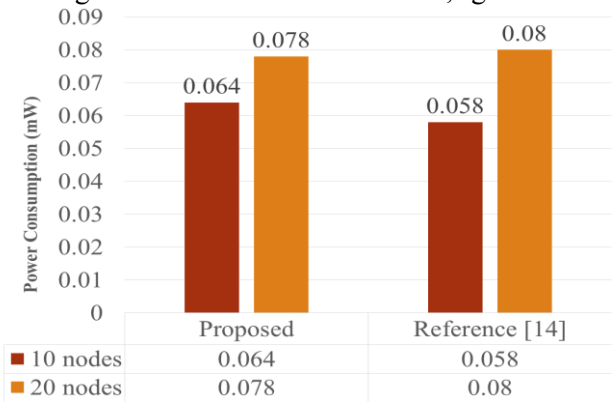

Fig.10 Comparison of power consumption with [14]

- Comparison of algorithm execution time:

Comparing the study with [12], we find that the proposed model is reducing the execution time of the algorithm that results in less delay and lower power consumption, so we can find that the proposed model offers a lightweight and fast security solution, fig.11.

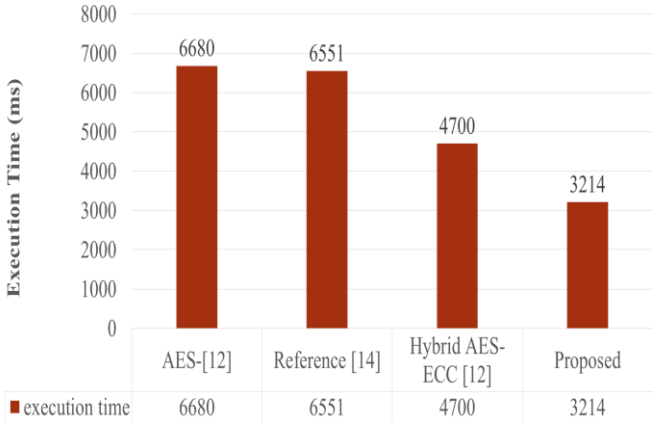

Fig.11 Comparison of the execution time of the algorithm with other studies [12-14]

4-5 Detection of the blackhole attack:

The attacking node aims to disrupt the service and steal the important information of the users. In the proposed model, the attack can be detected when a new node tries to join the network and obtain authentication, which will cause high-energy consumption, as in Fig.8. Also, the increasing number of packets with an attempt to join the network by an attacking node from Fig.7. When the attacking node is detected, it will be prevented from joining the

network, and encryption keys will be redistributed immediately from the sink node.
In addition, the attacking node will not be able to decrypt the data in the network due to the encryption process and the strength of the keys used.

5 Conclusions and recommendations

The model proposed in this paper helps to achieve secure integration between the Internet of Things and cloud computing using the hybrid encryption model (AES-ECC). To secure a reliable connection between the sensor nodes in the network and the cloud, store the sensor data securely, encrypted without affecting the packets delivery ratio, power consumption, and provide lower execution time compared to the others studies. The combined effect of both ECC and AES is appropriate for the proposed cloud storage technology to secure the system and helps to reduce storage volume with encrypted data.
This research aims to combine the availability of resources and maintain reliability and privacy when achieving the integration between the Internet of Things and cloud computing, and since each application has its requirements and conditions so this study is mainly directed to the Internet of Things networks with fixed and random publishing nodes in a field of study where data is collected from sensors and sent to the cloud to store them confidentially, Evaluate a set of parameters such as average power consumption, packet delivery ratio, and the algorithm execution time and compared to previous studies. The model can be used in many IoT applications that need speed, limited resources, and confidentiality in the transmission and storage of sensitive data.
However, the concept of security needs more study in the future to expand the concept of cloud computing through encryption technologies. In the future, this research could be improved by increasing the security of hybrid approaches by adding multiple layers of security to enhance system productivity and efficiency.

References:

[1]Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroiu, A. M. (2019), “Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges” Applied Computing and Informatics, Vol. ahead-of-print No. ahead-of-print, page 3.

[2]Rayes, A., and Salam, S., 2019, “Internet of Things from Hype to Reality_ the Road to Digitization” Second Edition, © Springer Nature Switzerland AG.

[3]Sokat, B., 2020, “Blackhole Attacks in IoT Networks" Master Thesis, Computer Engineering, Engineering and Sciences of İzmir Institute of Technology, İZMİR, 43p.

[4]Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., and Kayssi, A., 2016, “Identity-Based Authentication Scheme for the Internet of Things”, 978-1-5090-0679-3/16/$31.00 ©2016 IEEE.

[5]Ahmed, F., and Young-Bae Ko, 2016, “Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks”, Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1684

[6]HASSAN, A., ISMAIL, A., 2017, “Evaluation of encryption algorithms for IoT security” Bachelor of Science in Communication Engineering, Communication Engineering Department, University of almughtaribeen, Khartoum, Sudan, 49p.

[7]Langendoerfer, P., Piotrowski, K., Díaz, M. ,and Rubio, B., 2012, “Distributed Shared Memory as an Approach for Integrating WSNs and Cloud Computing” IEEE.

[8]Chenaru, O., Mihai, V., Popescu, D., and Ichim, L., 2018, Member, IEEE “Integration of WSN, IoT and Cloud Computing in Distributed Monitoring System for Aging Persons in Active Life” 26th Mediterranean Conference on Control and Automation (MED) Zadar, Croatia.

[9]Othman, M. M., El-Mousa, A., 2020, “Internet of Things & Cloud Computing Internet of Things as a Service Approach”, 2020 11th International Conference on Information and Communication Systems (ICICS), Amman, Jordan.

[10]Latif, I.H., 2020, “Time Evaluation Of Different Cryptography Algorithms Using Labview” 2020 IOP Conf. Ser.: Mater. Sci. Eng. 745 012039View

[11]Kunchok, T., Prof. Kirubanand V.B., 2018 "A Lightweight hybrid encryption technique to secure IoT data transmission"International Journal of Engineering & Technology, 7 (2.6) 236-240.
[12]Rehman, S., Bajwa, N.,Shah, M., Aseeri , A., and Anjum, A.,2021, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage" Electronics 2021, 10, 2673.
[13]Kumari C. S., Asha C. N., Rajashekhar U., K. Viswanath, 2022, "Performance Analysis of Cloud-based Health Care Data Privacy System Using Hybrid Techniques", International Journal Of Biology And Biomedical Engineering, Volume 16.
[14] Alzahrani, S.M., 2022, "Secure Authenticated Key Exchange For Enhancing The Security Of Routing Protocol For Low-Power And Lossy Networks", Master thesis of Science in Cyber Security, Wright State University.