International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

A Hybrid Cryptography Algorithm for WoT based on GOST and Speck

[1]Haider K. Hoomod [2]Jolan Rokan Naif [2] Israa S. Ahmed
1: Mustansiriyah University, College of Education, Computer Science dept.,
2: Informatic Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatic

Submitted: 10-08-2021 Revised: 25-08-2021 Accepted: 28-08-2021

ABSTRACT
In this paper is dedicated to present the design of the proposed Web of Things (WoT) security system, the proposed security for the WoT transmission data contains two steps: Encryption and the integrity and authentication data stage. The proposed security mechanism is designed and built using two lightweight algorithms (GOST and Speck) with many modifications in order to get more security and stall compatible with the WoT devices and sensing data in sending and receiving sensing data.

This proposed system provides a high level of security for any sensitive information that may be generated from sensors that may be installed in an important location to protect buildings and offices from theft by making certain modifications to the algorithms necessary to maintain the safety and security of the information, etc., which must be protected from Attacks or displayed by hackers. This system was designed to be successful in providing message content protection properties, including confidentiality, integrity, and authentication, and also to be compatible with all kinds of sensing data and sensors. This system is designed to be effective in providing security features for message contents that include confidentiality, authentication and non-repudiation, and is compatible with all types of remote sensing data and sensors to send the final notification to the final administrator view.

The proposed algorithm is designed to provide users with high flexibility and ease in managing change operations, speeding up encryption operations and intruding the contents of message packets (types and forms of different sensor data) at the point of origin and decrypting and checking packet integrity messages upon receipt. These features make users of this system more confident with each other.

I. INTRODUCTION

With the major advances in technology and electronics, the internet is connected to billions of computers. Every day, the number of devices connected to the network is increasing[1-3].

This increased use of Web of Things (WoT) has led to users starting to worry about the future in terms of information security which is one of the main challenges facing the evolution of these technologies. How to maintain the confidentiality, integrity, and authentication of that information during transmission[2,4,6].

This reason, many users have stopped using these technologies. Therefore, there have been many techniques and suggestions for maintaining the confidentiality, integrity, and authenticity of that information. [6,7]

Io T and WoT are display challenges in security relating that are determined by the IERC 2010 Strategic Research and Innovation Roadmap (SRIR). While some detailing is helpful, there are additional parts that needing to address by the research-society. Although there are numerous specific challenges of privacy, trust, and security in the IoT/WoT, they share many incidental non-functional requirements. [8,9]

The WoT offers real opportunities for wearable devices, smart homes, software, and information sharing via the Internet. Considering that the information that may be shared is private, maintaining the security of this information is a fundamental requirement in the Web of Things [10,11,12]. Addressing such obstacles is one of the continuing challenges that the Web of Things has to face Chandu Y and et al were used a hybrid algorithm that includes both algorithms (AES, RSA) to provided security data during transmission and storage of this data in the cloud. The proposed algorithm enables the Edge device to encrypt the data generated with AES before sending it to the cloud [13,14,21]. The AES key is encrypted using the RSA cipher system. The RSA encrypted key is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

exchanged with the authorized person via email[3,15,16].

Hayder Najm and et al were used a hybrid cipher method based on the GOST block algorithm and the Salsa (20) stream algorithm[4]. In order to be provided adequate security with randomly high hardness, it reinforces the five standard tests and modifies the key schedule as secure processes[17-20]

Haider K. Hoomod and et al were used the Speck-SHA3 (SSHA) algorithm resulting from a modification to the SHA-3 algorithm by replacing the KECCAK function with another very fast algorithm SPECK, which produces a very fast algorithm with a strong security level reliable in the validation of the data produced by the sensors [5,24,27,28]. Also, the extended logistic system is used to generate the initial values that the SHA3 algorithm uses to make these values unknown which the intruder cannot guess or recognize. This algorithm achieved SSHA, the speed was this algorithm much faster than the SHA-3 algorithm, with the ability to provide a good level of data security and integrity in a wot environment compared to the level of security provided by the original SHA-3 algorithm. Also, the SSHA algorithm could be used in IoT systems that need methods to quickly and securely verify data integrity[20-23].

In this paper, a hybrid encryption method will be proposed that based on the GOST algorithm and SPECK algorithm to provide confidentiality of information during it transmits from a source to the final interface, as well as the SHA-3 algorithm will be proposed in order to ensure that the information that may be received from WoT system is not falsified and its contents are not modified. In addition to validating this information.

II. THE PROPOSED SECURE WOT SYSTEM

The problem that is dealt with in this paper is the treatment of security problems that may arise when sending information via network, which may carry information on the Internet, which is responsible for monitoring the status of the halls or buildings in which it was installed. So, it is proposed a hybrid of modify the GOST algorithm and Speck algorithm to increase its security as well as to increase the speed of converting explicit media into encrypted media. This process also helped to preserve the information generated by the sensors and also prevented the hackers from viewing or modifying them.

The proposed system is based on the availability of alerts in response to the emergence of safe sensor data from the central workstation. The security mechanism is suggested to make the sensing data more secure through the network to connect the object sensors. The proposed system consists of five main layers (Sensing layer, Collection layer, sending layer, receiving layer and the response layer to the web decision making and displaying).

On the Sensing layer, which is explained as a data sensing layer, the sensors are distributed as clusters and each group contains (at least five sensors' devices). So, the sensors will be deployed in specific locations to read the situation or the surrounding environment by many parameters that will help to determine the decision by these parameters.

In the data collect/aggregates layer, the distribution of data collection devices on each set of sensors. So that, each set of sensors is controlled by the device like microcontroller (client side) through the wireless network.

In this proposed work, the microcontroller type that is used will be Raspberry pi3 that will have deployed and controlled on set of sensors. Raspberry Pi3 is also connected to the main (server-side) Raspberry that was used to send the collected sensor data to the computer responsible for parsing the sensor data and receiving the response.

The Third layer is the sending layer that required lightweight security mechanism. The Hybrid Proposed Security Mechanism (**HPSM**) consists of three stages: security chaos keys generation, sensing data encryption, and authentication. this stage will be used in proposed algorithms to provide the security and authentication to the data that is generated by sensing layer.

HPSM contains a range of modern encryption and authentication technologies that consist of many security algorithms that work together to achieve better security results. They are provided through a combination of security algorithms that work together and are interconnected in their work. They provide both encryption and data authentication by applying and implementing a modified encryption algorithm with each other and a set of new authentication strategy.

The WoT devices work with continuous numerical data that is generated continuously and at specified time intervals. This data must be secured using an advanced security mechanism. Each part of the IoT device must be secured with the appropriate security system.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

So, the proposed PSM consists of more than one algorithm integrated into a single security system (as shown in Figure 1), and these systems are:

1) 4D Chaos Keys Generation (using extended Lorenz system).
2) Authentication message by using SHA3.
3) Hybrid Modified Lightweight GOST-Speck Encryption Algorithm.

In authentication process, a set of algorithms will be used to produce a faster hash than the original algorithms are adopted. So, the SHA3 architecture was relied upon as the basis for building an algorithm for hashing production and a four-dimensional from chaotic system will be used to produce alternative primary values for values that will be replaced with the initial values of SHA3 algorithm.

Sensing data blocks encryption were done by two symmetric Lightweight algorithms (GOST-Speck) by using different chaos keys that will be produced from hyper chaotic system in both encryption and decryption, encryption of data using GOST-Speck provides confidentiality to the sensing data.

Chaos Keys Generation algorithm was used to generate random numbers by using a combination of the Extended Lorenz chaotic system with different initials and parameters values to produce 5D chaos keys values (used chaotic system from [27]. Chaos keys used in all HPSM algorithms: in generating their encryption/hash keys, and in some encryption/hashing functions.
In encryption stage, the proposed encryption algorithms (Hybrid GOST-Speck Algorithm (HGSA)) were used for the purpose of protecting sensor data in the WoT system.

The HGSA designed by merging the GOST algorithm (24 rounds) with the Speck algorithm (with 10 rounds) The rounds decreasing was for the purpose of reducing encryption time. Figure 1 illustrating a block diagram of the Hybrid GOST-Speck Algorithm. The Speck algorithm was inserted as a layer in the GOST round layers to avoid many attacks by increasing the strength and complexity of the GOST encrypting security results.

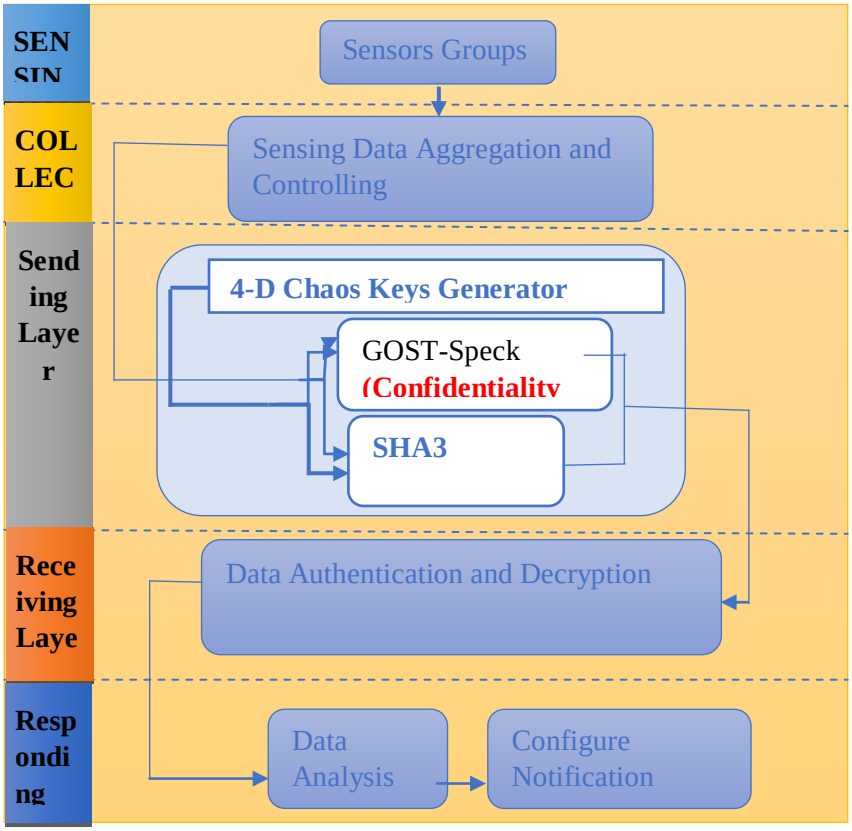

Figure (1): Block Diagram of the Proposed System Structure and Internal Algorithms.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

The steps of HGSA are as following:

1. Collect the sensors data from the data collection phase in the form of a TXT file, it enters to HGSA, where the following stages below show how HGSA works:
2. Divide collected data into blocks from 1024 bits, then divide 1024 bits into 512 bits for both sides (left and right).
3. Divides the 2048-bit secret key into eight parts from sub keys starting from K1, K2, ..., K5, so that each part is 1024 bits.
4. The total number of rounds for the HGSA is 28.
5. In each round, both from the right side and the left side are xored with 1024 bits keys.

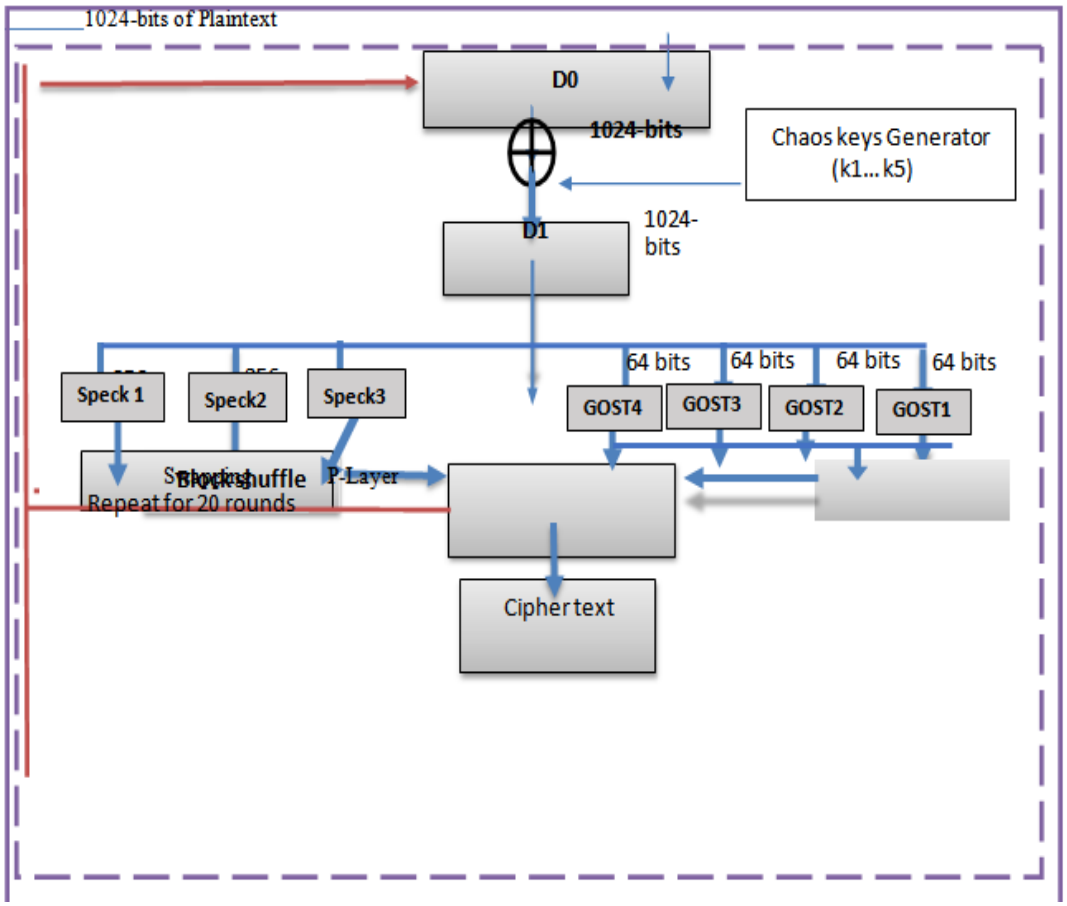

Figure (2) shows the structure of the proposed HGSA.

III. RESULTS AND DISCUSSION

The new proposed lightweight encryption algorithm called (HGSA) algorithm hybrid by the GOST and Speck algorithms. The proposed system deals with 1024 bits of data. The 1024 bits of data that entered into the system will be xoring with Chaos keys to result D1. Then the 1024 data bis splits into three parts of 256 bits entered to three Speck algorithms and four parts of 64 bits entered to four GOST algorithm. Results sides will be swapped and then repeat the previous operation to 20 rounds as illustrate in figure (2).

A standard NIST test will be used for testing HGSA encryption. Table (1) explains the timeline for the proposed encryption method on various sizes of file encryption.

Table (1): benchmarking performance of the HGSA (20rounds) average time (in msec) (using random data)

Operation	HGSA(1024bit)
Encryption (1 KB)	0.09076
Decryption (1KB)	0.1083

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

Encryption (10KB)	1.16233
Decryption (10KB)	1.01750
Encryption (100KB)	62.0098
Decryption (100KB)	63.6712
Encryption (1MB)	547.3420
Decryption (1MB)	545.6554
Encryption (10MB)	998.6321
Decryption (10MB)	995.1423

Table (2) illustratesthe results of NIST tests applied to the HGSA results to ensure it has better security to avoid and prevent various types of attacks.
The HGSA is passed through all NIST tests on each round (24 and20) due to its functions and chaos.

Table (2): NIST tests results of the HGSA-1024bit

NIST statistical tests Results Name	**HGSA 1024 bit**	
	Rounds	
	24	**20**
Frequency (Monobit) test	0.895	0.873
Runs test	0.995	0.960
Discrete Fourier transform	0.987	0.980
Block frequency	0.883	0.867
Longest runs test	0.950	0.949
Cumulative sums test	0.908	0.802
Serial test	0.987	0.975
Matrix rank test	0.792	0.770
Overlapping template test	0.954	0.943
Linear complexity test	0.979	0.962
Nonoverlapping template test	0.888	0.874

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1762-1769 www.ijaem.net ISSN: 2395-5252

Random excursions variant test	1.121	1.099
Random excursions test	0.998	0.987

Table (3) indicates the average HGSA 1024-bit encryption time with separate iteration rounds (24 and 20). 20-rounds HGSA 1024-bit encryption time is faster than rounds.

Table (3): the average encryption time for HGSA 1024-bit with different iteration rounds (24 and 20).

Text Size (KB)	**HGSA 1024-bit Time (msec) (24 Rounds)**	**HGSA 1024-bit Time(msec) (20 Rounds)**
1	**0.0203**	**0.0201**
10	**0.089**	**0.078**
25	**0.357**	**0.299**
75	**1.684**	**1.532**
100	**2.832**	**2.765**
1000	**8.785**	**8.654**
2000	**19.915**	**19.852**
10000	**100.784**	**100.427**
500000	**200.593**	**200.341**

The proposed HGSA algorithm has been constructed with fewer complexity functions (as seen in time calculation), although for various rounds, the CPU cycles are an average of between 8999 and 11407 cycles for different round cycles (encryption rounds and data size).

IV. CONCLUSIONS

The hybrid of the GOST and speck algorithms is a simple pointed issue for designing a strong encryption algorithm useful in many fields like IoT, WoT, WSN, media encryption etc. hybrid combination as shown in results has a certainty circumstance in avoiding the weak in the two algorithms, this the weak point of the method of cryptanalysis as related-key cryptanalysis. However, this resolved by the proposed method (Gost -Speck) to have the right combination and more robustness security. This hybrid algorithm deals with 1024-bit input data block and 2048-bit chaos keys. Its need for 21^{256} probable keys to breaking keys that, because of its uncomfortable procedure in this situation, is to be not used brute force attack. Also, the proposed hybrid algorithm passed the all NIST standard tests successfully with best of the randomness.

REFERENCES

[1]. S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo, "Security Analysis of a Cryptographically-Enabled RFID Device.," in USENIX Security Symposium, 2005, vol. 31, pp. 1–16.

[2]. T. W. Cusick, C. Ding, and A. R. Renvall, Stream ciphers and number theory. Elsevier, 2004.

[3]. S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT

2015. pp. 1577–1581, 2016, doi: 10.1109/ICGCIoT.2015.7380718.

[4]. H. Najm, H. K. Hoomod, and R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," Periodicals of Engineering and Natural Sciences, vol. 8, no. 3. pp. 1829–1835, 2020, doi: 10.21533/pen.v8i3.1619.

[5]. H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "Modify Speck-SHA3 (SSHA) for Data Integrity in Wot Networking Based on 4-D Chaotic System," Period. Eng. Nat. Sci., vol. 8, no. 4, pp. 2379–2388, 2020, doi: 10.21533/pen.v8i4.1743.

[6]. Y. Chandu, K. S. Rakesh Kumar, N. V. Prabhukhanolkar, A. N. Anish, and S. Rawal, "Design and implementation of hybrid encryption for security of IOT data," Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017. pp. 1228–1231, 2018, doi: 10.1109/SmartTechCon.2017.8358562.

[7]. E. M. Ludmila Babenko, "Algebraic Cryptanalysis of GOST Encryption Algorithm." Journal of Computer and Communications, 2014.

[8]. M. Hell, T. Johansson, A. Maximov, and W. Meier, "A stream cipher proposal: Grain-128," in 2006 IEEE International Symposium on Information Theory, 2006, pp. 1614–1618.

[9]. Y. Minglin and M. Junshuang, "Stream ciphers on wireless sensor networks," in 2011 Third International Conference on Measuring Technology and Mechatronics Automation, 2011, vol. 3, pp. 358–361.

[10]. L. Babenko, E. Ishchukova, and E. Maro, "GOST encryption algorithm and approaches to its analysis," Theory and Practice of Cryptography Solutions for Secure Information Systems. pp. 34–61, 2013, doi: 10.4018/978-1-4666-4030-6.ch002.

[11]. K. L. Tonni Limbong1, Janner Simarmata2, ARS Tambunan2, Parulian Siagian3, Joel Panjaitan4, Lestina Siagian3, Erbin Sitorus4, Marvin Frans Sakti Hutabarat5, Abba Suganda Girsang6, "The implementation of computer based instruction model on Gost Algorithm Cryptography Learning." IOP, 2018.

[12]. A. P. U. S. Muhammad Iqbal1, Yudi Sahputra2, "The Understanding of GOST Crytography Technique." International Journal of Engineering Trends and Technology (IJETT) – Volume 39 Number 3- September 2016 The, 2016.

[13]. R. Rahim, S. Suprianto, and M. T. Multazam, "GOST enhancement key processing with Triple Transposition Key," Journal of Physics: Conference Series, vol. 1402, no. 6. 2019, doi: 10.1088/1742-6596/1402/6/066093.

[14]. R. R. Heri Nurdiyanto, "Enhanced Pixel Value Differencing Steganography with Government Standard Algorithm." International Conference on Science in Information Technology (ICSITech), 2017.

[15]. L. Babenko, E. Ishchukova, and E. Maro, "Research about strength of GOST 28147-89 encryption algorithm," Proceedings of the 5th International Conference on Security of Information and Networks, SIN'12. pp. 138–142, 2012, doi: 10.1145/2388576.2388595.

[16]. R. A. F. Lustro, A. M. Sison, and R. P. Medina, "Performance analysis of enhanced speck algorithm," ACM International Conference Proceeding Series. pp. 256–264, 2018, doi: 10.1145/3288155.3288196.

[17]. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, and B. Weeks, "Notes on the design and analysis of Simon and Speck," IACR Cryptology ePrint Archive. p. 560, 2017.

[18]. M. A. Abdelraheem, G. Leander, and E. Zenner, "Differential Cryptanalysis of Round-Reduced SPECK Suitable for Internet of Things Devices." pp. 1–17, 2011.

[19]. 5Student Anil G. Sawant, 2Sayali Kamthe, 3Yashasvini Shaha , 4Bapu Morajkar , 5Abhishek Sakpal *1 Research Scholar (Asst. Professor) , 2Student, 3Student, 4Student and *1, "Implementation of SIMON & SPECK Algorithm.pdf." Journal of Emerging Technologies and Innovative Research (JETIR), 2019.

[20]. H. K. Taehwan Park, Hwajeong Seo, "Parallel Implementations of SIMON and SPECK.pdf." IEEE, 2016.

[21]. M. Salih Mahdi and N. Flaih Hassan, "a Suggested Super Salsa Stream Cipher," Iraqi J. Comput. Informatics, vol. 44, no. 2, pp. 1–6, 2018, doi: 10.25195/2017/4422.

[22]. A. K. Farhan, "Proposed Hybrid Approach of Stream Cipher Base on Selector of Encryption operation and Key Symmetric Translate," vol. 29, no. 11, 2011.

[23]. F. T. Abd El Hussien, "Proposed Algorithm To Generate Encryption Key For Block And Stream Cipher Using DNA Computing," Iraqi Journal of Information Technology,

vol.8, no. 3, pp. 68-82, 2018, doi: 10.34279/0923-008-003-008.

[24]. Jolan Rokan Naif Al-Khazraji, Ghassan H.Abdul-Majeed and Alaa Khadhim Farhan "Design And Implementation Of Secure IoT for Emergency Response System Using Wireless Sensor Network and Chaotic", Ph.D. dissertation , Iraqi commission for computers and informatics , informatics institute for postgraduate studies, 2019.

[25]. Ahmed Majed, Haider Kadhim Hoomod:" Secure Email of Things Based on Hyper Chaotic system", Al-Mustansiriyah University, Baghdad, Iraq, M.Sc. Thesis ,2020.

[26]. Hoomod, Haider K., and A. M. Radi. "New Secure E-mail System Based on Bio-Chaos Key Generation and Modified AES Algorithm." In Journal of Physics: Conference Series, vol. 1003, no. 1, p. 012025. IOP Publishing, 2018.

[27]. Kubba, Zaid M. Jawad, and Haider K. Hoomod. "A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System." In 2019 First International Conference of Computer and Applied Sciences (CAS), pp. 199-203. IEEE, 2019.

[28]. Hoomod, Haider K., Jolan Rokan Naif, and Israa S. Ahmed. "Modify Speck-SHA3 (SSHA) for data integrity in WoT networking based on 4-D chaotic system." Periodicals of Engineering and Natural Sciences (PEN) 8, no. 4 (2020): 2379-2388.