Improving Security of IoT Devices using Cryptographic Algorithms

Reece B. D'Souza[1], Yash Priyadarshi[2]

[1]Student, School of Computer Science and Engineering, Vellore Institute of Technology, Tamil Nadu, India
[2]Student, School of Computer Science and Engineering, Vellore Institute of Technology, Tamil Nadu, India

---***---

Abstract - *IoT has revolutionized the Smart Home Environment with all of its features, tools, and technologies, and its easily modifiable and scalable environment. The use of Internet of Things (IoT) devices has become very common these days, being present in almost every home. Internet of Things (IoT), to define it, is a huge network of interconnected gadgets which can gather data of the surroundings in which they operate. As this technology requires a connection to the internet, data transfer among components may not always be secure. This insecure data may be subject to attack at any moment. To prevent this, the use of cryptographic algorithms is necessary. But to the low processing power of an IoT Processor, conventional cryptographic algorithms may be deemed too heavy a burden on the performance. Therefore, the use of lightweight cryptography is required. Lightweight Cryptography, much like conventional cryptography, encrypts and decrypts data using specific algorithms and with the use of a key. The differences are only in the performance and optimization. Lightweight cryptography runs much faster than conventional. This lightweight cryptography may sometimes lack security. Therefore, the paper proposes the hybridization of a conventional algorithm and a lightweight algorithm. This algorithm will possess a high performance in terms of execution time.*

Key Words: IoT (Internet of Things), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard), Lightweight, Hybrid, Cryptography, Performance

1. INTRODUCTION

The use of Internet of Things (IoT) devices has become very common these days, being present in almost every home. Internet of Things (IoT), to define it, is a huge network of interconnected gadgets which can gather data of the surroundings in which they operate. A simple example of an IoT device is a smoke detector, a device that is present in many homes. The term IoT was first coined by the British Technology Pioneer, Kevin Ashton in the year 1999. He had coined this term while he was working in an Auto-ID Lab Centre, and was referring to a global network of RFID or Radio-Frequency Identification connected objects.

Since 1999, this technology has been on the rise and has been dominating the market for smart solutions to everyday problems. It has the capability of collecting small amounts of data continuously for a large duration and can process it and give specific feedback to other devices that are connected to it. It can also communicate among other devices using specific modules, remotely as well as locally. These devices are generally connected to the internet and communicate through that medium.

The Internet of Things has been a hot topic for quite some time and now more than a few billion people are interconnected through it. Due to this, it may be possible to steal various kinds of data from regular people. Perpetrators can easily use this stolen data for any illegal activities. Therefore, securing this data is of the utmost importance.

Cybersecurity, while not new to the field of IoT, has been gaining some traction. Due to the rise in awareness of data theft among normal citizens, there is also a rise in the development of security initiatives and programs in IoT. Normally, since IoT devices only possess a portion of the performance of a Personal Computer (PC), the use of heavy-weight encryption algorithms on IoT devices can severely affect their performance and operation. Therefore, the use of lightweight cryptography is needed.

Lightweight cryptography consists of several cryptography algorithms developed for implementation in constrained environments such as IoT sensors and devices and their environment [2]. It delivers a good count of security. All the original types and ideas of cryptography still apply to lightweight cryptography. The only difference is in the frequency of rounds of encryption and the size of the input and output data when compared to heavyweight cryptography.

Two main reasons that support the use of Lightweight Cryptography Algorithms are mentioned as follows. One is the efficiency of end-to-end communication Conventional Cryptography algorithms cannot be applied to limited powered or battery-powered devices as their power consumption rate is high. Therefore, the use of lightweight cryptography algorithms is necessary. The other is the applicability to lower resource devices. The footprint of conventional cryptography algorithms is far more than the lightweight algorithms and thus would open up various possibilities of connections with lower resource devices. With this ideology, the implementation of lightweight cryptography algorithms can be deemed fruitful in terms of power consumption, CPU load, execution time, etc.

2. LITERATURE SURVEY

A literature survey was performed among papers of the same topic and beyond it to list out the features and shortcomings of the paper and hence the subject.

The paper by S. Surendran, A. Nassef, and B. D. Beheshti, explains how lightweight cryptography is meant for extremely resource-constrained devices and they are used not only for encryption purposes but also for authentication and hashing under highly resource-constrained devices [1]. The article starts by explaining various cryptography algorithms after which the authors explain the attacks on lightweight ciphers. Lastly, a performance comparison in terms of execution time is shown for the algorithms chosen. A major drawback is that this article has not proposed any algorithm, only a comparative study between different algorithms has been analyzed and shown as the results.

The paper by J. S. Kumar and D. R. Patel displays various applications of the Internet of Things and how this domain is gaining success in Cyber Security and Privacy control domains [2]. Various applications discussed are healthcare, smart home, and intelligent community security system (vehicle management system, surrounding security subsystem, property management). Lastly, security and privacy concerns related to IoT have been discussed. One drawback is that this article is thoroughly theoretical and explains mainly about applications of the Internet of Things. No implementational model has been proposed on how to improve the existing security systems.

The paper by W. Iqbal and H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, suggests that with the increase in the number of IoT devices, there has been a tremendous increase in the amount of data to be processed and analyzed [3]. When such large data are processed there is a high risk of threats and security issues to the IoT devices in use. This article reviews the threats, challenges, attack vectors of IoT networks and their security requirements. A combination of network-based IoT architecture and Software Defined Networking has been proposed. Finally, to provide security solutions a detailed overview of Software-Defined Security has been explained. The framework proposed by the authors for countermeasure is very big and computationally extensive due to which the implementation cannot be carried out on a large number of devices having less performance power.

A comparative analysis was conducted by M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, in terms of power consumption, throughput, energy performance, and time consumption of various algorithms including DES, AES, MD5, SHA, and RSA [4]. All these algorithms have been run on Raspberry Pi and Arduino. Although, All the algorithms used for analysis are heavyweight and have been implemented before and no innovation towards lightweight cryptography has been discussed.

The article by M. Abomhara and G. M. Køien classifies threat types, analyzes them, and characterizes the intruders and attacks on IoT devices and their services [5]. The ACID properties have also been discussed after which various security threats, attacks, and vulnerabilities of IoT devices have been up. Lastly, the authors have discussed intruders and organized groups for attacks. The article is a survey on various threats and vulnerabilities on IoT networks. It was focused on security challenges on IoT devices and services and failed to provide a real-time solution for the classified attacks.

The article by A. Arabo is focused on analyzing the risks associated with smart devices in a smart home network and the challenges faced while maintaining the security of the same [6]. The authors have done threat assessments and formulated a table containing the terms threat, threat vector, and security measures. The threats taken into account are data exfiltration, tampering, data loss, and malware for which threat vectors and security measures have been explained. No testbed has been provided for their proposed analysis on how to address the increasing threats.

Similar to the paper by M. El-Haii [4], the article by A. Dhatrak, A. Sarkar, A. Gore, M. Paygude, M. Waghmare, and H. Sahane is focused on studying the security threats on IoT devices and providing countermeasures for the found threats [7]. Also, the authors have discussed the applications of the Internet of Things like medicine, health care, smart city, business, and automotive. Although, no implementational model has been provided for their research.

A. Safi proposes a hybrid encryption algorithm to reduce safety risks and the time consumption in doing the same with less computational complexity [8]. They have formulated the algorithm keeping in mind overall perception, intelligent processing, and reliable transmission. For data exchange in IoT focus has been given toward integrity, non-repudiation, and confidentiality. Lastly, they have used MATLAB software to test the speed and efficiency of their proposed algorithm. The proposed algorithm has made a hybrid of HAN, AES, and RSA algorithms all of which are very heavyweight and make the system overheat after running continuously.

Y. Lu and L. D. Xu review cybersecurity in the Internet of Things in a systematic manner [9]. The key factors associated with their work are the protection and integration of smart devices having different functionality and information communication technologies. Their research is applicable in the cybersecurity of IoT, its architecture and taxonomy, and finally strategies and countermeasures for attacks and vulnerabilities in an IoT network system. The article could have explained how intrusion detection and prevention could have been incorporated while designing a smart home network. Also, for authentication and verification purposes, 2FA could be very helpful.

The article by L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwainder explains the background of IoT systems and their security measures [10]. The identification of various security and privacy issues has been discussed. The approach and techniques for having a secure IoT environment have been discussed which also includes the improvement of existing solutions. A new IoT layered model has been proposed which improves the privacy and security components, and the identification of the layer. The authors could have used lightweight cryptography methods to improve the power constraint factor and for the execution of their model on devices with lesser performance power.

V. A. Thakor, M. A. Razzaque, M. R. A. Khandaker deals with resource-constrained devices like sensors, smart cards, RFID tags, etc. which have limited processing power, low memory, limited energy usage, or a combination of all of these in their paper [11]. To make the communication by these devices more secure, lightweight cryptography has been suggested and compared in terms of time consumption, memory usage, latency, key and block size, energy efficiency, and hardware efficiency. The paper made lightweight algorithms for pre-existing algorithms and no hybridization was proposed.

Similar to the article by A. Safi [8], the article by J. Bugeja, A. Jacobson, and P. Davidson has presented an overview of security and privacy challenges on IoT networks [12]. The difference is that the article was focused on the broader area of IoT whereas this article is focused on the smart home domain. The constraints have been identified, solutions have been evaluated and challenges have been discussed in this article for the privacy and security issues. Although, the article did not provide an implementation model for the proposed solution based on the survey conducted.

The main focus of the algorithm proposed by M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan is given to healthcare systems [13]. This article proposed a new cryptography algorithm called Galois protocol which was used to encrypt confidential data coming from different medical sources. To embed the encrypted data to a low complexity image steganography technique was used. To optimize the selection of cover blocks within an image Adaptive Firefly algorithm was used. The final algorithm formulated is very computationally extensive and would be optimized using lightweight cryptography algorithms.

The article by N. Komninos, E. Philippou, and A. Pitsillides is based on any issues related to the Smart Grid and Smart Home's security [14]. The threats that are detected are then categorized according to specific security goals set for the smart home/smart grid environment. An evaluation is made on the impact of the overall system security. Countermeasures for the same are also focused on in this research article. Similar to the paper by M. El-Haii, M. Chamoun, A. Fadlallah and A. Serhrouchni [4] and A. Dhatrak, A. Sarkar, A. Gore, M. Paygude, M. Waghmare, and H. Sahane [7], an intrusion prevention system could be installed in the smart grid network and for validation of the authentic used 2FA could also be used here as well.

The article by N. Komninos, E. Philippou, and A. Pitsillides is based on any issues related to the Smart Grid and Smart Home's security [14]. The threats that are detected are then categorized according to specific security goals set for the smart home/smart grid environment. An evaluation is made on the impact of the overall system security. Countermeasures for the same are also focused on in this research article. Similar to the paper by M. El-Haii, M. Chamoun, A. Fadlallah and A. Serhrouchni [4] and A. Dhatrak, A. Sarkar, A. Gore, M. Paygude, M. Waghmare, and H. Sahane [7], an intrusion prevention system could be installed in the smart grid network and for validation of the authentic used 2FA could also be used here as well.

3. PROPOSED SYSTEM MODEL

The Hybrid Algorithm is made with the combination of AES, SPECK, and PRESENT Algorithms. The reason the previously mentioned were chosen where their strengths in being either lightweight or highly secure and cryptographic. Therefore, the novel algorithm is lightweight without compromising any aspect of security.

3.1 Key Generation

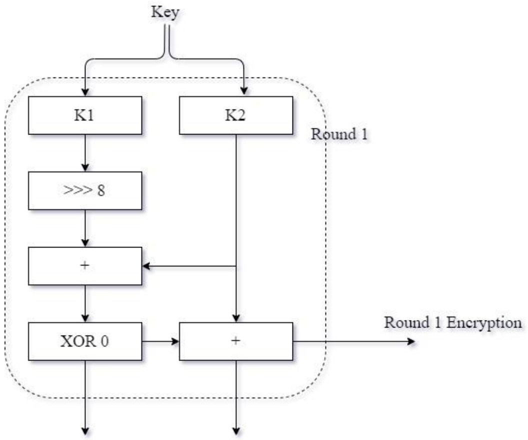

Fig -1: Hybrid Algorithm Key Generation Function

The key generation procedure is as follows:

1. The key is split into two halves: K1 and K2.
2. In each round (11 rounds in total):
   a. K1 undergoes an 8-bit right shift
   b. Addition with K2
   c. XOR'd with 0
   d. K2 undergoes addition with the output of c
   e. The output of d is the key that will be used in the Encryption Procedure
3. The output of K1 and K2 received from each round acts as the input for the next round.
4. Thus, the keys are generated.

3.2 Encryption

The encryption procedure is as follows:

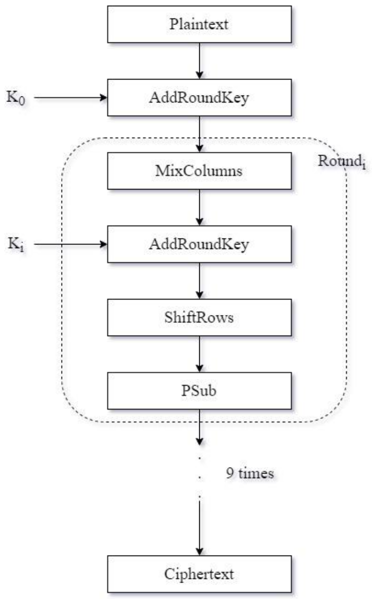

Fig -2: Hybrid Algorithm Encryption Function

1. The plaintext (PT) is fed into the algorithm. It is 64-bit in length
2. The AddRoundKey() is performed with the PT and Key0 from the key generation procedure and the output is termed as a 'state' variable.
3. In each round (for a total of 10 times):
   a. Mix Columns: This step belongs to the AES Algorithm. Here, similar to the AES Algorithm, each column of the 64 bits is transformed into new bytes using a special mathematical function. For every column:
      i. Assign the column into a temporary variable.
      ii. Each column is multiplied by the following Matrix:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

   b. AddRoundKey: This step belongs to the PRESENT Algorithm. Here, the 64-bit value of the 'state' and the 64-bit Key for that round are XOR'd.
   c. Shift Rows: This step belongs to the AES Algorithm. Here, similar to the AES Algorithm, each state undergoes the following operations:
      i. The first row remains unchanged
      ii. The second row is shifted to the left by one position
      iii. The third row is shifted to the left by two positions
      iv. The fourth row is shifted to the right by one position
   d. PSub: This step belongs to the PRESENT Algorithm. Here, similar to the PRESENT Algorithm, each element is permuted to position in the PBox values from the PRESENT Algorithm. The PBox values are presented in Table 1.

Table -1: Permutation Box for PRESENT Algorithm

i P(i)	0 0	1 16	2 32	3 48	4 1	5 17	6 33	7 49
i P(i)	16 4	17 20	18 36	19 52	20 5	21 21	22 37	23 53
i P(i)	32 8	33 24	34 40	35 56	36 9	37 25	38 41	39 57
i P(i)	48 12	49 28	50 44	51 60	52 13	53 29	54 45	55 61
i P(i)	8 2	9 18	10 34	11 50	12 3	13 19	14 35	15 51
i P(i)	24 6	25 22	26 38	27 54	28 7	29 23	30 39	31 55
i P(i)	40 10	41 26	42 42	43 58	44 11	45 27	46 43	47 59
i P(i)	56 14	57 30	58 46	59 62	60 15	61 31	62 47	63 63

4. After 10 rounds in total, the state variable is the ciphertext.

3.3 Decryption

The procedure for decryption is the exact reverse of the encryption process.

1. For decryption, the ciphertext is 64-bit in length.
2. In the process of decryption, the order of each round is as follows:
   a. Inv Mix Columns: This step belongs to the AES Algorithm. Here, similar to the AES Algorithm, each column of the 64 bits is transformed into new bytes using a special mathematical function. For every column:
      i. Assign the column into a temporary variable.
      ii. Then each column is multiplied by a matrix:

$$\begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}$$

b. AddRoundKey: This step belongs to the PRESENT Algorithm. Here, the 64-bit value of the 'state' and the 64-bit Key for the round (10 - Roundi) are XOR'd.

c. Inv Shift Rows: This step belongs to the AES Algorithm. Here, similar to the AES Algorithm, each state undergoes the following operations:

   i. The first row remains unchanged

   ii. The second row is shifted to the right by one position

   iii. The third row is shifted to the right by two positions

   iv. The fourth row is shifted to the left by one position

d. InvPSub: This step belongs to the PRESENT Algorithm. Here, similar to the PRESENT Algorithm, each element is permuted to position in the PBox values from the PRESENT Algorithm. The PBox values are presented below in Table 2.

Table -2: Inverse Permutation Box for PRESENT Algorithm

i	0	1	2	3	4	5	6	7
P(i)	0	4	8	12	16	20	24	28
i	16	17	18	19	20	21	22	23
P(i)	1	5	9	13	17	21	25	29
i	32	33	34	35	36	37	38	39
P(i)	2	6	10	14	18	22	25	30
i	48	49	50	51	52	53	54	55
P(i)	3	7	11	15	19	23	26	31
i	8	9	10	11	12	13	14	15
P(i)	32	36	40	44	48	52	56	60
i	24	25	26	27	28	29	30	31
P(i)	33	37	41	45	49	53	57	61
i	40	41	42	43	44	45	46	47
P(i)	34	38	42	46	50	54	58	62
i	56	57	58	59	60	61	62	63
P(i)	35	39	43	47	51	55	49	63

3. Finally, the key0 is added using the AddRoundKey() function.

4. The state variable obtained is the original plaintext.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling

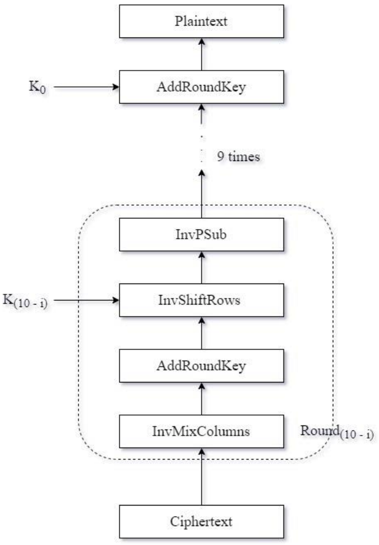

Fig -3: Hybrid Algorithm Decryption Function

4. RESULTS ANALYSIS

The following results were obtained after running the algorithms on a simulation Arduino UNO using the Proteus Professional Software. The execution time was calculated using the micros() function.

4.1 Encryption Execution Time

Table -3: Encryption Execution Time of all algorithms

Algorithm	Execution Time (in μs)
DES	~17600
AES	~12800
3DES	~52800
Hybrid	~750

The above table can be viewed graphically through the chart given below.

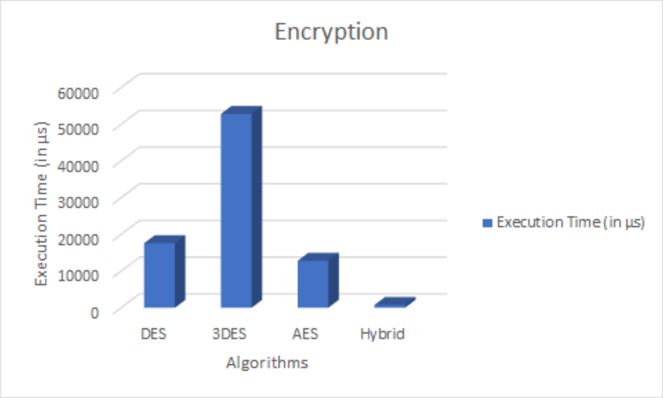

Chart -1: Encryption Execution Time

4.2 Decryption Execution Time

Table -4: Decryption Execution Time of all algorithms

Algorithm	Execution Time (in µs)
DES	~17600
AES	~13000
3DES	~52800
Hybrid	~1200

The above table can be viewed graphically through the chart given below.

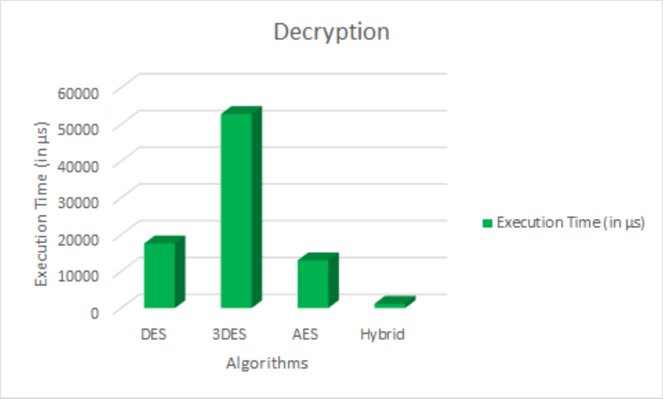

Chart -2: Decryption Execution Time

5. CONCLUSIONS

As clearly visible from Chart -1 and Chart -2, the Hybrid Algorithm's encryption and decryption execution times are significantly lesser than the conventional algorithms. The CPU Load when the Hybrid Algorithm is being executed is also quite significantly lower than when the other conventional algorithms are executed.

This is due to the addition of several lightweight features in a normal heavyweight algorithm, such as reduction in the number of rounds, reduced size of substitution boxes, and optimization of C++ code.

The following setup was run in an Arduino Environment, but the results would hold the same for any other microprocessor environment (Eg. Raspberry Pi).

REFERENCES

[1] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices," 2018 IEEE Long Island Systems, Applications, and Technology Conference (LISAT), 2018, pp. 1-8, DOI: 10.1109/LISAT.2018.8378034

[2] J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887), Volume 90, No 11, March 2014

[3] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security", IEEE Internet of Things Journal, Vol. 7, No. 10, October 2020

[4] M. El-Haii, M. Chamoun, A. Fadlallah and A. Serhrouchni, "Analysis of Cryptographic Algorithms on IoT Hardware platforms," 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 1-5, DOI: 10.1109/CSNET.2018.8602942

[5] M. Abomhara, and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security and Mobility, 2015, Vol. 4, pp. 65-88

[6] A. Arabo, "Cyber Security Challenges within the Connected Home Ecosystem Futures", Procedia Computer Science, 2015

[7] A. Dhatrak, A. Sarkar, A. Gore, M. Paygude, M. Waghmare, and H. Sahane, "Cyber Security Threats and Vulnerabilities in IoT", International Research Journal of Engineering and Technology, 2020, Vol. 07, No. 03

[8] A. Safi, "Improving the Security of Internet of Things Using Encryption Algorithms", International Journal of Computer and Information Engineering, 2017, Vol. 11, No. 5

[9] Y. Lu, L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103-2115, April 2019, DOI: 10.1109/JIOT.2018.2869847

[10] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwainder, "IoT Privacy and Security: Challenges and Solutions", Applied Sciences. 2020, Vol. 10, No. 12

[11] V. A. Thakor, M. A. Razzaque, M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison, and Research Opportunities", IEEE Access, 2021, Vol. 9

[12] J. Bugeja, A. Jacobson and P. Davidson, "On Privacy and Security Challenges in Smart Connected Homes", 2016 European Intelligence and Security Informatics Conference

[13] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, "Securing Data in the Internet of Things (IoT) Using Cryptography and Steganography Techniques", IEEE Transactions on Systems, Man, and Cybernetics: Systems, January 2020, Vol. 50, no. 1, pp. 73 – 80

[14] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures”, IEEE Communication Surveys & Tutorials, Vol. 16, No. 4