Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 2, May 2021, pp. 1191~1198
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i2.pp1191-1198

Analysis and evaluation of symmetric key ciphers for internet of things smart home

Lujain S. Abdulla[1], Musaria K. Mahmood[2], Abbas F. Salih[3], Sulaiman M. Karim[4]
[1]Department of Electrical Engineering, College of Engineering, Tikrit University, Tikrit, Iraq
[2]Department of Electrical and Electronics Engineering, İstanbul Gelisim University, İstanbul, Turkey
[3]High Institute of Infertility Diagnosis and Assisted Reproductive Technologies, Al- Nahrain University, Baghdad, Iraq
[4]Department of Computer Engineering, Karabuk University, Karabuk, Turkey

Article Info

Article history:

Received Dec 31, 2020
Revised Mar 22, 2021
Accepted Apr 11, 2021

Keywords:

AES
DES
IoT
SAFER+
TDES

ABSTRACT

A large number of sensors and intelligent devices are interconnected via the internet to collect data as part of the internet of things (IoT) applications. Data security is one of the important challenges for these applications due to vulnerability of the internet. IoT devices limiting factors, such as delay-sensitivity, restricted memory, and low computing capability, make choosing the appropriate data encryption standard extremely important. The current research focuses on evaluating four data security, block cipher standards for the IoT smart home application. Considering the encryption/decryption speed, DES, TDES, AES, and SAFER+ standards are evaluated by implementing the algorithms with MATLAB to determine the best security solution. The simulation of the four standards shows the superiority of SAFER+ standard in term of encryption speed compared to others added to its capabilities on security, and software implementation opportunity. The use of classical symmetric key standards for real time data security in the IoT application can be validated through the selection of SAFER+.

Corresponding Author:

Musaria Karim Mahmood
Department of Electrical and Electronics Engineering
Istanbul Gelisim University
Cihangir, Şehit Jandarma Komando Er, J. Kom. Er Hakan Öner Sk. No:1, 34310 Avcılar/İstanbul
Email: mkmahmood@gelisim.edu.tr

1. INTRODUCTION

Nowadays, internet of things (IoT) has become a trait of the modern technology era where things are interconnected to produce intelligent systems that use the Internet as a communication infrastructure. Besides low computing power, short-range communication, limited bandwidth and memory capacity, data security is the most important challenge in the IoT devices [1], [2]. Applying same security techniques that exist in the information technology (IT) system introduces time-delay defying the real-time system performance requirement [3]. The security challenges surrounding the IoT are reviewer in [4] by summarizing all potential attacks targeting infrastructure and devices. Technology, trends, and solutions available in the market are surveyed for IoT authentication, access control, and trusted management. Several studies have suggested authentication using an asymmetric key standard rather than full data encryption for IoT applications [5]. Although the delay introduced by this standard is greater than that by symmetric key standard, it can be justified by using it only once at the start of data collection. Other works suggest using lightweight encryption as a low-power, memory-efficient encryption standard that requires low computing power [6]. In [7], [8], two comprehensive reviews have been conducted on the literature relating to encryption standards

used for IoT applications. The reviews concluded that classic encryption standards like AES, DES, RSA and TDES cannot be used efficiently due to their complex implementation requiring large memory and high computing facilities. A performance comparison between the advanced encryption standard (AES) and the extended tiny encryption algorithm (XTEA) for IoT applications is given in [9]. XTEA is a lightweight encryption standard while AES is a traditional encryption standard for IT. Results show that XTEA outperforms AES in term of power consumption, memory requirements, and software implementation but the latter is proved to be more secure. Before exchanging data between different devices in an IoT environment, a lightweight authentication procedure is introduced in [10]. It is based on the dynamic cipher combined with asymmetrical public key encryption in a client-server model application. In [11], both costumer authentication and data encryption is developed for healthcare applications. The process starts by an authentication using biometric parameters in addition to username and password. Data encryption is accomplished through two standards, namely, substitution-ceaser cipher and the improved elliptical curve cryptography (IECC). Comparison of the proposed system with a similar procedure consisting of authentication by rivest-shamir-adleman (RSA) and an encryption by ECC shows its improved performance in terms of encryption speed and average correlation coefficient. The biggest security-related challenge for the IoT system is the vulnerability against IT-likely cyber attacks that promotes the use of similar countermeasures for data protection [12]. Although traditionally IT security standards require more computing capability, they provide stronger encryption than lightweight standards [13]. AES qualities for IoT security implementation are approaching in many researches as in [14], [15]. Most of these works are investigating the use of simplified version of the original AES algorithm by modifying some of the encryption/decryption steps that make it a lightweight block symmetric standard. In [16], the secure and fast encryption routine (SAFER++) is presented for securing IoT applications. It is a low-complexity, secure, and fast block cipher, accomplished by modifying the original SAFER standard with a 64-key length resulting in an algorithm that is equally secure but simpler. The objective of this research is the performance evaluation of the data encryption/decryption speed of DES, TDES, AES, and SAFER+ standards by software implementation for IoT-smart home application. The article is organized as follows: the methodology is presented in the Section II. The implementation results are shown in the in Section III. Section IV concludes the article.

2. RESEARCH METHOD

2.1. IoT-smart home and security challenges

IoT aims to connect device-to-device, person-to-device, and person-to-person, and thus it provides the connection between things and heterogeneous networks for many applications such as the industrial IoT, IoT-health care, and IoT for smart home and smart city [17, 18]. The data is used for monitoring, controlling and allowing specific actions to be automatically activated whenever certain situations arise. IoT smart home like other applications, is characterized by the use of sensor-device with limited memory and computing power resulting a security strategy far from using IT encryption standards known by their complex structures. To overcome this limitation, a security model is proposed based on local server as outlined in the Figure 1. Data is collected by sensor-device and send via in-house Ethernet to a local server where the necessary computing and memory requirement for using classical IT encryption are presents. The local server is connected to the Internet via a gateway-firewall as part of the strategy of ring of defense [19]. This strategy includes many security measurements such as antivirus, firewall, data encryption and authentication process as shown in the Figure 2. This work evaluates the possibility to adopt a minimum-delay classical IT symmetrical key encryption standard for the data encryption layer.

2.2. Encryption standards

The selection of DES, TDES, AES, and SAFER+ standards as candidate is logically justified by their efficiency and wide spreading in various IT applications. The DES and TDES are developed by IBM and known since the beginning of the seventies as the approved data encryption standard for data communication [20]-[22]. The AES is the most used block encryption standard for IT systems known by its high performances in a variety of platforms in term of encryption time, avalanche effect, low power consumption and memory requirement [21], [23]. It is always used as comparison reference for other standards in all data encryption applications [24], [25]. SAFER+ algorithm is a member of SAFER cipher family which was first proposed as candidate for the AES standard [26]. Recently it has brought attention by its good performances in hardware-software implementation, high encryption/decryption speed, and good resistance against various attacks [27], [28]. SAFER encryption is adopted as the basic component for Bluetooth communication security [29], [30]. The main characteristics of the selected standards are given in Table 1.

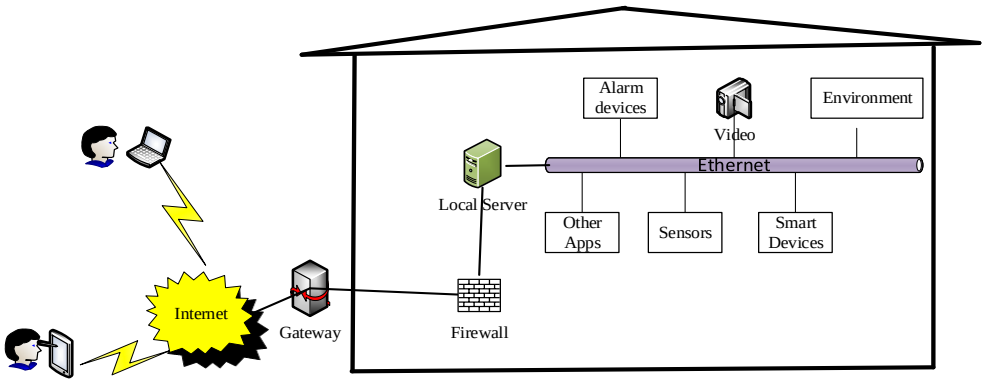

Figure 1. IoT smart home security

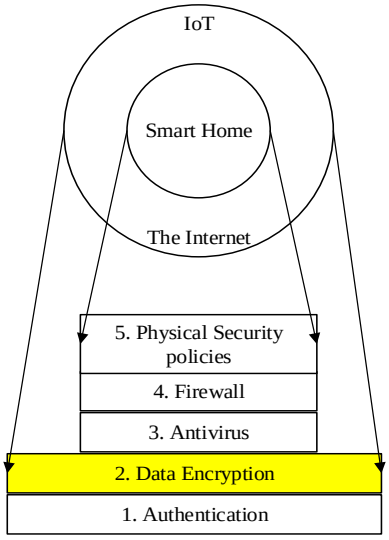

Figure 2. Ring of defense

Table 1. Standards performances

Factor	DES	3DES	AES/ Rijndael	SAFER+
Cipher type	Symmetric	Symmetric	Symmetric	Symmetric
Key length	56	168	128, 192, 256	128, 192, 256
Block size	64	64	128	128
Published	New, 1977	1995	2000	1999
Structure	Feistel	Feistel	Substitu.,Permuta.	Substitu.,Permuta.
Possible keys	1	1	1	1
Security	Weak	Good	High	High
Cryptanalysis resistance	Brute Forced	Brute Forced	Brute Forced	Brute Forced

2.2.1. DES

Plaintext of 64-bit length is encrypted by 16 rounds using 56-bit key length based on Feistel network principles. The initial secrete key is given to both encryption side and decryption side as 64-bit key, but by removing 8 bits the key size is decreased to 56-bit key. The 8^{th} bit is used as parity check for the 7 bits that preceded it in the sequence of the original key. Every round is using a reduced sub-key of 48-bit length generated from the original key by a key schedule through many permutation and selection procedures. The sub-key generation procedure shows weak randomized operations which are reflected as reduced cipher complexity. The input 64-bit plaintext block is subject to initial permutation according to fixed input-output switching procedure and then divided into two groups L_0 and R_0, each of 32-bit. Data and sub-key are then processed in the 16 rounds by Feistel network as shown in the figure 3 where the details of the first round are given. The DES algorithm employs many predefined tables for data encryption operations like substitution,

compression, expansion, inversion, and breakdown [20], [21]. The decryption algorithm is based on the reverse mathematical operations to regenerate the original plaintext from an encrypted data. There are many improved versions of the DES that tried to overcome the security limitation especially against brute force attacks such as double-DES and TDES which are based on the same principles with repeated encryption rounds. TDES is proposed to resolve the weakness in DES without designing a full new cipher algorithm [22]. To resist to the brute-force attacks, TDES algorithm is using a key of 168 bits (3 times 56) to perform three successive block encryption operation similar to that in the DES algorithm. The total effective encryption rounds are 48 rounds while the decryption is implemented by 48 reverse-process round.

2.2.2. AES

Rijndael algorithm have been selected as the AES by NIST in 2001 among several encryption candidates to be the official standard [9], [31]. Data are encrypted-decrypted on 128-bit blocks using a secret key of three options, 128, 192, or 256 bits' length. The number of rounds depends on the key length such that 10 rounds is used the case of 128-bit key, 12 rounds for 192-bit key, while for the option of 256-bit key there are 14 rounds. Data encryption results from mathematical operations over the entire data block in every round in an iterative process while in the DES part of data is subject to Feistel cipher in each round. Round input data goes through four-bit and byte operations; sub-byte, shift-row, mix-column, and add-round-key as depicted in the Figure 4, where N is the number of rounds. The last encryption round is based on only three operations which are sub-byte, shift-row, and add-round-key. A predefined S-box of 16×16 values is used to generate the substitution of an input byte by another one according to mapping procedure. The output byte location on the s-box is found by dividing the input byte into two 4-bit groups, where the left indicates the row number and the right shows the column index. Blocks are then distributed on four groups of four bytes each. The first group is unchanged, the second is circularly shifted to the lift by one byte, two similar bytes are shifted for the third group, and three byte-shift is applied for the last group. The mix-columns operation is a matrices multiplication using the prime polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Finally, the 128-bit key is XOR added bit-by-bit to the data to produce the round output data. The key schedule is based on the division of the secret key on four words, each with four bytes. One sub-key is generated for every encryption round using a XOR addition with byte rotation to lead a good randomizing process by applying nonlinear operations. Decryption algorithm uses same principles shared by all block ciphers by providing an inverse operation for every encryption step [14].

2.2.3 SAFER+

SAFER+ is a 128-bit block cipher with three optional key lengths; 128-bit key, 192-bit key, or 256-bit and encryption/ decryption rounds (R) equal to 8, 12 and 16 accordingly [19], [27]. The protocol starts by the key schedule to generat a set of 2R keys from the original secret key owned by both sender and receiver sides (K_1). The 2R+1 keys group is used for encryption rounds as two keys per round, starting from K_1 to K_{2R} and the final key K_{2R+1} for the output encryption layer. The decryption side employs the reverse order by beginning from K_{2R+1} for the input decryption layer and then two keys per round as shown in the Figure 5. The key schedule uses byte number expansion, three bits left rotation, bytes selection, and matrix multiplication. SAFER+ round includes two linear transformation layers, a nonlinear layer, and finish by byte multiplication with the matrix M. Linear layers are based on byte-to-byte addition modulo 256 (add) and bit-by-bit addition operation (xor) of the layer 128-bit input data block with one of the round keys. The nonlinear layer uses a byte transformatiom on exponential and logarithmic function base (45) modulo 257 defined for the byte B by:

$$F(B) = \begin{cases} 45^B \ mod\ 257 & if\ B \neq 128 \\ 0 & if\ B = 128 \end{cases} \quad (1)$$

$$G(y) = \begin{cases} log_{45}(y) & if\ y \neq 0 \\ 128 & if\ \ y = 0 \end{cases} \quad (2)$$

M is a predefined invertable (16×16) matrix used as base for the final transformation stage in every round to ensure the fast diffusion and to make the algorithm resistant to differential cryptanalysis [32]. The decryption process begins with the input transformation layer operating on the ciphertext and the key K_{2R+1} with a subtraction (sub) as the inverse operation of add and xor operation in opposite locations of their peer operations in the output encryption layer. Two keys from the remaining 2R keys are used in decreasing order for rounds decryption. An inverse operation of that in the encryption is performed in every step of the decryption process.

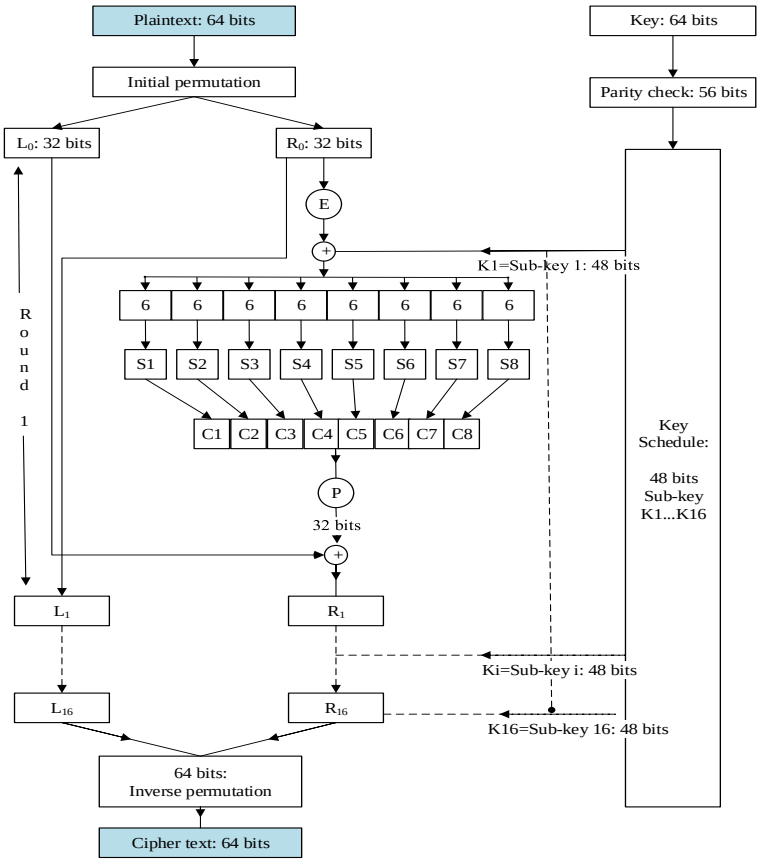

Figure 3. DES Encryption round

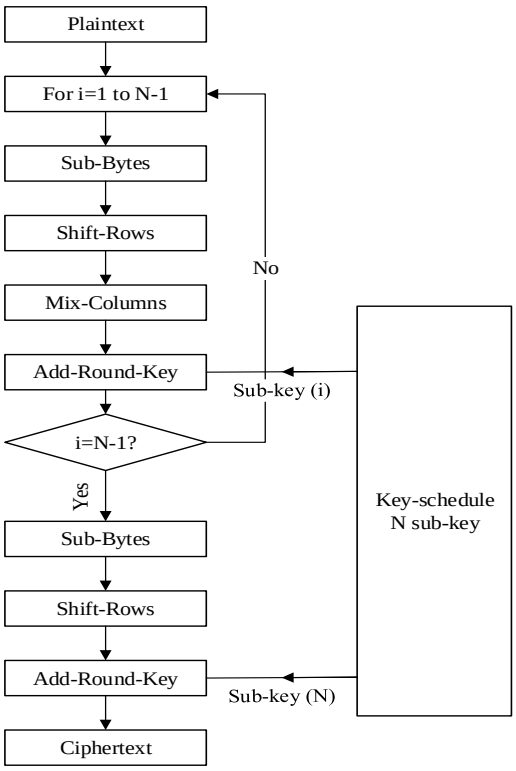

Figure 4. AES algorithm

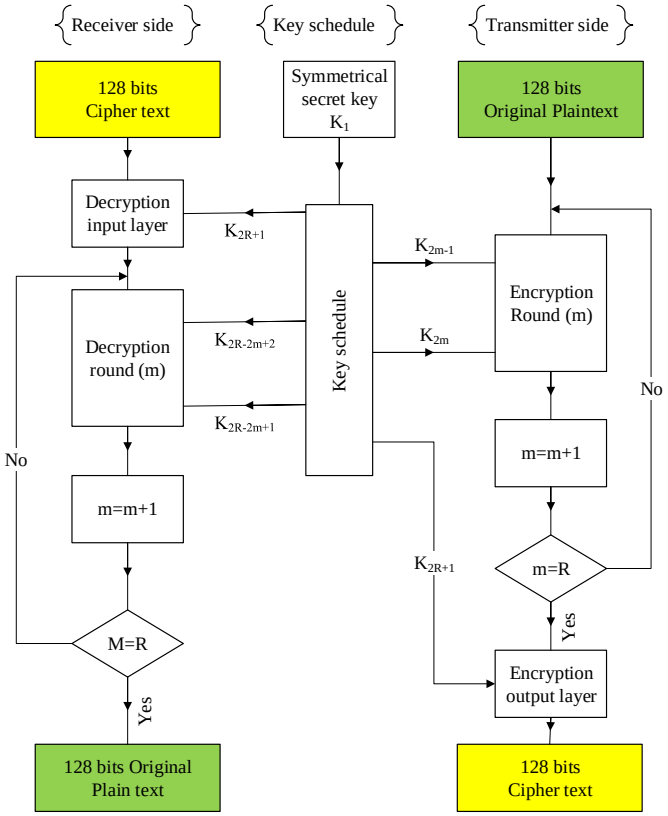

Figure 5. SAFER+ encryption/decryption

3. RESULTS AND DISCUSSION

Although MATLAB is considered a slow programming language; it can give a comparative study between various encryption standards. The performance of the four algorithms DES, TDES, AES, and SAFER+ is evaluated based on the delay introduced by the encryption/decryption procedures. SAFER+ is proven to be a faster than the other three standards as shown in Table 2. The software implementation is performed by the same tools and programmer for different file size ranging from 8 KB to 512 KB. The behavior of encryption/decryption time is linear with the data size for the four algorithms but with different slops as presented in Figure 6. The curve slops for the encryption procedure calculated from collected data are 9.7, 28.7, 27.7, and 2.1 for DES, TDES, AES, and SAFER+ respectively. This proves that SAFER+ is not only faster but is suitable for encryption of large amount of data. Similarly, the decryption time is linear with improved characteristics for the SAFER+ compared to the others. The data collection is pushed to 30.2 MB for SAFER+ to validate their linear characteristics in terms of encryption and decryption time.

Table 2. The performance of Cipher Standards

Data size	Time of DES (ms)		Time of 3DES (ms)		Time of AES/ (ms)		Time of SAFER+ (ms)	
(kB)	Encryp.	Decryp.	Encryp.	Decryp.	Encryp.	Decryp.	Encryp.	Decryp.
8	160	67	316	232	267	496	45	33
16	157	98	398	343	419	971	48	54
32	261	166	659	554	770	1904	61	60
64	501	338	1292	1117	1662	3667	161	140
128	1015	664	2652	2419	3502	7243	214	210
256	2042	1333	5627	4875	6593	16044	409	403
512	4135	4002	10902	9651	14182	33304	832	825
1024	10482	5819	21495	19469	27817	64660	1647	1653
2048	19923	14962	56424	46536	59067	128615	3404	3409
5120	48715	33773	147157	122674	141823	329205	10715	10330
10240	X	X	X	X	X	X	23043	22952
20480	X	X	X	X	X	X	41769	40678
30720	X	X	X	X	X	X	70826	69180

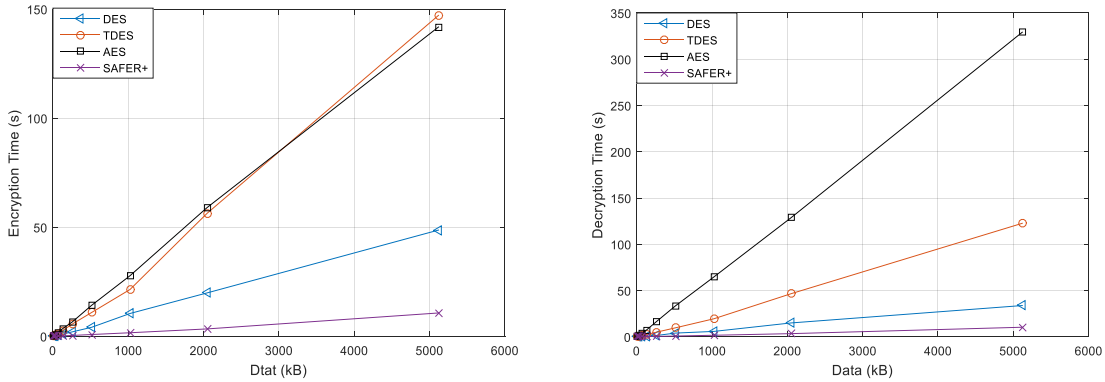

Figure 6. Encryption & decryption times.

4. CONCLUSION

IoT applications are real-time in nature which makes encryption/decryption time the central factor for selecting a suitable encryption standard. IoT-smart home application uses limited memory, and limited computing power devices, making it difficult to use the classic IT encryption standard for data security. The proposed local server-based architecture overcomes these limitations of IoT devices that contribute to the potential use of classic IT coding standards. The data is collected from different locations in the smart home operation area, and send to the local server via the in-house Ethernet network. The local server is protected by the ring of defense strategy and is used as a contact point with the outside network (Internet). To select an appropriate IT encryption standard for IoT smart home application, a study was condicted to evaluate the performance of four cryptographic standards known for their strong data security, namely, DES, TDES, AES and SAFER +. The software evaluation shows that SAFER+ outperforms others in term of operational delay and suitability for big data encryption. Simulations prove that for a file of 5.12MB, SAFER + is at least five times faster than its closest competitor in this group with a linear increase of time with encrypted file size.

REFERENCES

[1] R. Kumar, P. Khan and S. Kumar, *"A Cellular Automata-based Healthcare Data Encryption Technique for IoT Networks* ", 2019 IEEE 16th India Council International Conference (INDICON), Rajkot, India, pp. 1-4 , 2019, doi: 10.1109/INDICON47234.2019.9030349

[2] A. Khanum, Rekha V., "An enhanced security alert system for smart home using IOT", *Indonesian Journal of Electrical Engineering and Computer Science, Vol*. 13, No.1, pp. 27-34, Jan 2019, doi: 10.11591/ijeecs.v13.i1.pp27-34

[3] S. M. Errapotu, *et al*., "SAFE: Secure Appliance Scheduling for Flexible and Efficient Energy Consumption for Smart Home IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4380-4391, Dec. 2018. doi: 10.1109/JIOT.2018.2866998

[4] A. Jurcut, T. Niculcea, P. Ranaweera and Nhien-An Le-Khac, "Security Considerations for Internet of Things: A Survey", SN Computer Science, Article number: 193, 2020, doi: 10.1007/s42979-020-00201-3

[5] T. Song, *et al*., "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844-1852, 2017, doi: 10.1109/JIOT.2017.2707489

[6] M. Rana, *et al*., "A secure and lightweight authentication scheme for next generation IoT infrastructure", *Computer Communications*, Vol. 165, pp. 85-96, January 2021, doi: 10.1016/j.comcom.2020.11.002

[7] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil and Muhammad, "A Review of Data Security and Cryptographic Techniques in IoT based devices", *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems -ICFNDS* '18, June 2018.

[8] M. S. Mehmood, *et al*., "A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment," *2019 8th International Conference on Information and Communication Technologies (ICICT)*, Karachi, Pakistan, pp. 54-59, 2019.

[9] S. Maitra, D. Richards, A. Abdelgawad and K. Yelamarthi, "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy," *2019 IEEE Sensors Applications Symposium (SAS)*, Sophia Antipolis, France, pp. 1-6, 2019, doi: 10.1109/ICICT47744.2019.9001945

[10] A. Sachan, D. N. Kumar and A. Adwiteeya, "Light Weighted Mutual Authentication and Dynamic Key Encryption for IoT Devices Applications," *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, GHAZIABAD, India, pp. 1-6, 2019.

[11] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," *IEEE Access*, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739
[12] X. Chen, Y. Liu, H. Chao and Y. Li, "Ciphertext-Policy Hierarchical Attribute-Based Encryption Against Key-Delegation Abuse for IoT-Connected Healthcare System," in *IEEE Access*, vol. 8, pp. 86630-86650, 2020, doi: 10.1109/ACCESS.2020.2986381
[13] D. Richards, A. Abdelgawad and K. Yelamarthi, "How Does Encryption Influence Timing in IoT?," *2018 IEEE Global Conference on Internet of Things (GCIoT)*, Alexandria, Egypt, pp. 1-5, 2018.
[14] J. H. Anajemba, C. Iwendi, M. Mittal and T. Yue, "Improved Advance Encryption Standard with a Privacy Database Structure for IoT Nodes," *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, Gwalior, India, pp. 201-206, 2020.
[15] M. Dao, V. Hoang, V. Dao and X. Tran, "An Energy Efficient AES Encryption Core for Hardware Security Implementation in IoT Systems," *2018 International Conference on Advanced Technologies for Communications (ATC)*, Ho Chi Minh City, pp. 301-304, 2018.
[16] X. Guo, J. Hua, Y. Zhang and D. Wang, "A Complexity-Reduced Block Encryption Algorithm Suitable for Internet of Things," *IEEE Access*, vol. 7, pp. 54760-54769, 2019, doi: 10.1109/ACCESS.2019.2912929
[17] D. Shin, K. Yun, J. Kim, P. V. Astillo, J. Kim and I. You, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks," *IEEE Access*, vol. 7, pp. 142531-142550, 2019.
[18] T. S. Gunawan, et al., "Prototype Design of Smart Home System using Internetof Things", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 7, No.1, July 2017, pp. 107-115, doi: 10.11591/ijeecs.v7.i1.pp107-115
[19] M. K. Mahmood, and F. M. Al-Naima, "Developing a Multi-Layer Strategy for Securing Control Systems of Oil Refineries," *Wireless Sensor Network*, Vol. 2, No. 7, pp. 520-527, 2010, doi: 10.4236/wsn.2010.27064
[20] I. Sumartono and A. P. U. Siahaan, "Encryption of DES Algorithm in Information Security", *International journal for innovative research in multidisciplinary field*, Vol. 4, Issue 10, Oct. 2018.
[21] P. Patil, P. Narayankar, N. D G and M. S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", *Procedia Computer Science*, 78, pp. 617 – 624, 2016.
[22] H. O. Alanazi, *et al*., "New Comparative Study Between DES, 3DES and AES within Nine Factors", *Journal of computing*, volume 2, issue 3, pp. 152-157, March 2010.
[23] S. Chari, C. Jutla, J.R. Rao and P. Rohatgi, "A cautionary note regarding evaluation of AES candidates on smart-cards", *Proceedings of the second AES Candidate Conference*, pp. 133–147, March 1999.
[24] C. A. Lara-Niño, M. Morales-Sandoval and A. Díaz-Pérez, "An evaluation of AES and present ciphers for lightweight cryptography on smartphones," *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, Cholula, pp. 87-93, 2016.
[25] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms", *International Journal of Digital Technology & Economy*, Volume 1, No. 2, pp. 127-134, 2016.
[26] S. Mukherjee, D. Ganguly and S. Naskar, "A New Generation Cryptographic Technique", *International Journal of Computer Theory and Engineering*, Vol. 1, No. 3, pp.284-286, August, 2009.
[27] I. S. Ashour, "On Line Data and Voice Encryption System Based on FPGA Technology," *2007 National Radio Science Conference*, Cairo, pp. 1-7, 2007.
[28] A. Schubert and W. Anheier, "Efficient VLSI implementation of modern symmetric block ciphers," *ICECS'99. Proceedings of ICECS '99. 6th IEEE International Conference on Electronics, Circuits and Systems (Cat. No.99EX357)*, Pafos, Cyprus, vol.2, pp. 757-760, 1999.
[29] J. Padgette, K. Scarfone and L. Chen, "Guide to Bluetooth Security", *National Institute of Standards and Technology*: Gaithersburg, MD, USA, 2012.
[30] Y. Shaked and A. Wool, "Cracking the Bluetooth PIN*", proceedings of the 3rd USENIX/ACMConf. Mobile Systems, Applications, and Services (MobiSys)*, 2005.
[31] A. Kubadia, D. Idnani and Y. Jain, "Performance Evaluation of AES, ARC2, Blowfish, CAST and DES3 for Standalone Systems: Symmetric Keying Algorithms," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, pp. 118-123, 2019.
[32] M.F. Şahin, M. K. Mahmood, I. Myderrizi, "Secure and Fast Encryption Routine+: Evaluation by Software Application", *International journal OF engineering technologies-ijet*, Vol.6, No.2, pp.13-24, 2020.