ANALYSIS OF KEY GENERATION METHODOLOGY FOR THE INTERNET OF THINGS USING TRANSFORM-BASED FUNCTION

Mrs.B Sindhuja, Mr P Niranjan Reddy, Mr S Mahanthappa, Mr.M Satish, Mrs. Swetha Madireddy, Mrs.Pachimatla Divya, Mrs.Namilikonda Prathyusha, CMR Institute of Technology Hyderabad

ABSTRACT

The interoperability of the internet of things requires secured communication between source to IoT devices. The primary concern of security deals in the physical layer and network layers. The network layer security implementation is more costly than the physical layer security of the internet of things. Therefore, most authors focus on physical layer security based on transform-based functions to generate session keys between source and IoT devices. This paper proposed DCT based efficient secured communication-based session key generation method for IoT devices. The proposed algorithms minimized the signal pre-processing phase to convert multi-bit. The validation of the proposed algorithm simulates the IEEE 802.11 radio protocol in MATLAB. As a result, the proposed algorithm is more efficient instead of the existing algorithms.

Keywords: - IOT, RSSI, DCT, cryptography, 802.11, WSN, Communication.

INTRODUCTION

The Internet is a technology that played an important role in the transformation of the world to its current state. Now the Internet has reached a state that it is not even recognized as a service, but a part of the environment around us. The broad ap plications of Internet came into its peak as every-thing around us are connected to each other and become part of some network. Now, the situation has reached where any-thing can be ‘smart’ or ‘digital’. The ‘Internet of Things’ conceptualizes the world which has all the things around you are having some kind of digital identity and part of some network, communicating and sharing information [1,2]. The Internet of Things (IoT) refers to an ever-growing network comprising the objects which are not just traditional computers or mobile devices, but the physical entities like watches, wearable devices, and other smart objects. It can be considered as a network or interconnection of sensors and actuators having a unique framework for information sharing. The IoT doesn’t stick to any specific protocol but is open to any state-of-the-art protocol available now and enhance the range to the maximum. Further, the management of data and network can be automated and the efficiency can be increased using the M2M interactions when all the devices become smart. Even the user inputs can be automated with sensors and the solutions will be communicated directly to the things where it is supposed to happen [3,4]. This change in the concept from connected computers to a network of ‘things’ revolutionized the digital world and created a fresh wave of development. The idea of digital identity and connectivity to each entity has increased the influence of Internet to another extent. With the wireless connectivity and new digital identification techniques like RFID, the IoT got its clutches over their daily life [4,5,6]. Advancements in Wireless Sensor Networks (WSN) and low power, resource constrained devices have increased the type of devices that can be connected to the Internet. Moreover, the IPv6 and IEEE 802.15.4 have been significant to provide more addresses and accommodate more components and net-works into the world of IoT. As shown in the below figure, these recent technologies have been fundamental in transforming the Internet to the Internet of Things [7,8,9]. The rest of paper describe as in section II. Process of key generation. In section III describe the proposed methodology. In section IV experimental analysis and finally conclude in section V.

II. KEY GENERATION

Various key generation algorithms used transform function and signal quantization methods in wireless communication. The channel parameters such as RSS used in case of key generation and key extraction for IoTs device. The Skyglow algorithms used DCT transform function for the process of quantization and enhance the reliability of bit and reduce the bit error rate (BER). The Skyglow algorithm reduces the utilization of radio frequency in case of receptions and transmissions. These algorithms not used the process of privacy amplification for the generation of key [10,11,12,13]. The generated key length of Skyglow is 128 bits. The Key entropy of Skyglow is very high and enhances the reliability of IoTs based communication system. Some authors used key generation system five stages and some are used four steps. The steps of key generation shown in figure 2. The 1st step of process measures the channel properties b/w 2 authorized party. The measured difference's value is high then used the process of preprocessing. The next step is quantization of signals into bit single bit value and multi-bit value. After the process of quantization measured the bit difference value is called error correcting phase and finally proceed for the privacy amplification. In privacy amplification used the hash code algorithm for the creation of message digest[14,15,16].

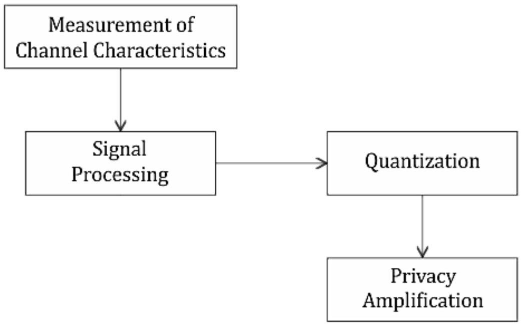

Figure1 : Process of key generation algorithms using Five phase.

III. METHODOLOGY

The proposed keys generation algorithm based on three steps as follows channel reciprocity, quantization and amplification. The reduces steps of proposed algorithm, increase the computational and time efficiency of communication model. The proposed algorithm applied the discrete wavelet packet transform for the process of quantization and multiresolution mapping of bit sequence. The process of exchange of information share by cyclic key. The cyclic key is lightweight public cryptography approach for the amplification of message. The proposed algorithm describe here[18].

```
Algorithm:
Input: RSS channel characteristic $Y_u$
          The formation variation of RSS signal T
          The bit formation of RSS M
          The length of bit N
Output: the sequence of keys: [0101010…]
     1.  Assign the number of node $2^k$
     2.  Estimation of M bit in each node with $W_T$ [$P_1$, $P_2^K$]
     3.  For 1← i to n do
          If $Y_{ui} \leq T- (T/n)$ ││ node-1
          If $N_{ui}=P_1$
          Else $T-(T/n)<Y_{ui}<T$ ││ node-2
                    $Nu=P_2$
          Else if $T<Y_{ui} + (T/n)$ ││ node-3
          Else if $Y_{ui}\geq T + (T/n)$ ││ node-4
```

```
        $N_i=P_4$
    End if
        M = [$P_1$, $P_2$, $P_3$, $P_4$…………]
    End for
```

IV Experimental Analysis

To evaluate the performance of proposed algorithm of secret key generation simulated in MATLAB software with version R2014a. MATLAB software provides various function of modulation and sampling of RSS signals. The configuration of system I7 processor 8GB RAM and windows 10 operating system. The simulation scenario in MATLAB design in phase of indoor and outdoor with condition of obstacle and other signal attenuation process. The carrier frequency of RSS signal is 2.45GHZ. the process of simulation work in half-duplex mode of communication. the interval of RSS signal measure on time interval 110ms. The distance of two communicating device with interval of 10, 20, 40, 50 and 60 centimeters. For the validation of algorithms measure following standard parameters[19,20].

1. Bit Error Rate (BER): BER denotes the bit mismatch prob-ability between two generated keys.
2. Key Agreement Rate (KAR): KAR denotes the probability of generating identical keys with no bit errors.
3. Key Leakage Rate (KLR): KLR denotes the probability of Eve reconstructing the key using the unencrypted syndrome.
4. Key Entropy: The generated key should be random, thus, with an entropy that is ideally 1.
5. Secret Bits per Packet (SBP): SBP denotes the number of generated bits per message exchange between the communicating parties. SBP is a proxy for energy-efficiency.

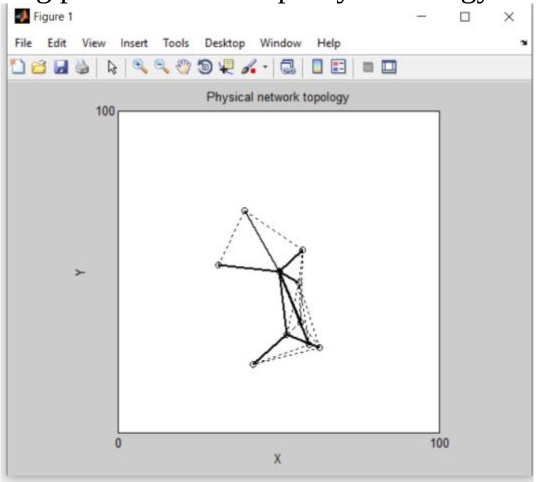

Figure 2: Window show that the physical network topology with x-axis and y-axis of an efficient generation method for IoTs using DWT and DCT. Here hit the DCT technique.

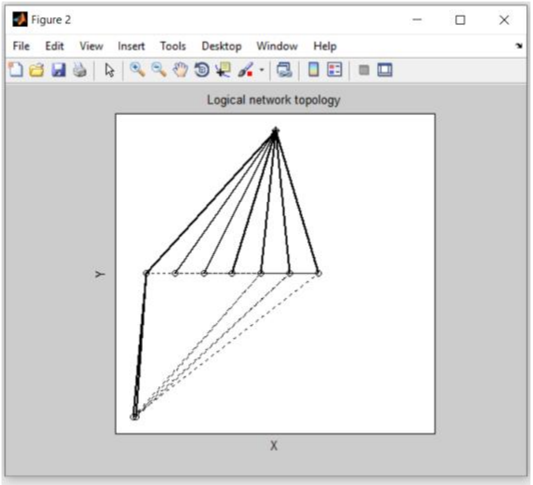

Figure 3: Window show that the physical network topology with x-axis and y-axis of an efficient generation method for IoTs using DWT and DCT. Here hit the DCT technique button.

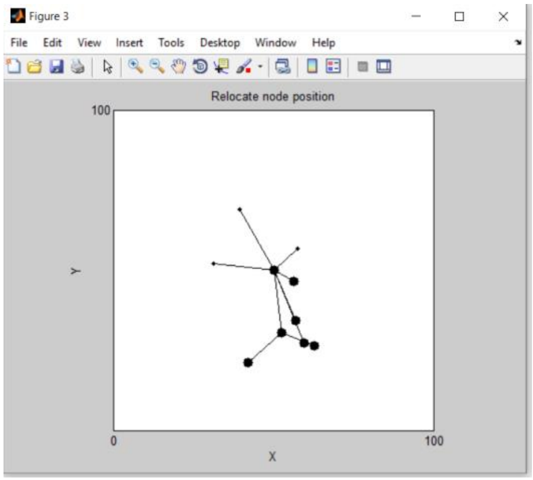

Figure4 : Window show that the relocate node position with x-axis and y-axis of an efficient generation method for IoTs using DWT and DCT. Here hit the DCT technique button.

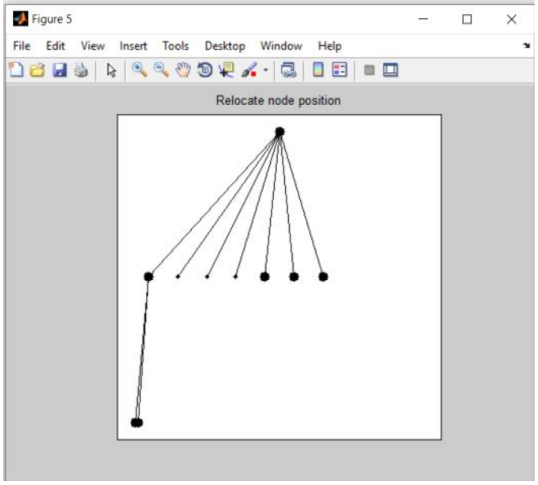

Figure 5: Window show that the relocate node position with x-axis and y-axis of an efficient generation method for IoTs using DWT and DCT. Here hit the DCT technique button.

Table 1: Comparative performance of DCT, DWT, Skyglow and proposed with these parameters BER, KAR, KLR, Entropy.

	DCT	DWT	Skyglow	Proposed
BER	0.58	0.59	0.57	0.55
KAR	0.83	0.84	0.86	0.88
KLR	0.005	0.005	0.007	0.007
Entropy	0.89	0.90	0.92	0.88

Table 2: Comparative performance of DCT, DWT, Skyglow and proposed with these parameters BER, KAR, KLR, Entropy.

	DCT	DWT	Skyglow	Proposed
BER	0.64	0.64	0.66	0.63
KAR	0.78	0.79	0.78	0.80
KLR	0.007	0.006	0.006	0.008
Entropy	0.84	0.88	0.84	0.82

Table 3: Comparative performance of DCT, DWT, Skyglow and proposed with these parameters BER, KAR, KLR, Entropy.

	DCT	DWT	Skyglow	Proposed
BER	0.70	0.68	0.69	0.67
KAR	0.58	0.60	0.59	0.61
KLR	0.005	0.006	0.007	0.007
Entropy	0.84	0.88	0.84	0.82

Table 4 : Comparative performance of DCT, DWT, Skyglow and proposed with these parameters BER, KAR, KLR, Entropy.

	DCT	DWT	Skyglow	Proposed
BER	0.71	0.71	0.71	0.72
KAR	0.80	0.81	0.82	0.82
KLR	0.007	0.006	0.007	0.008
Entropy	0.79	0.79	0.78	0.80

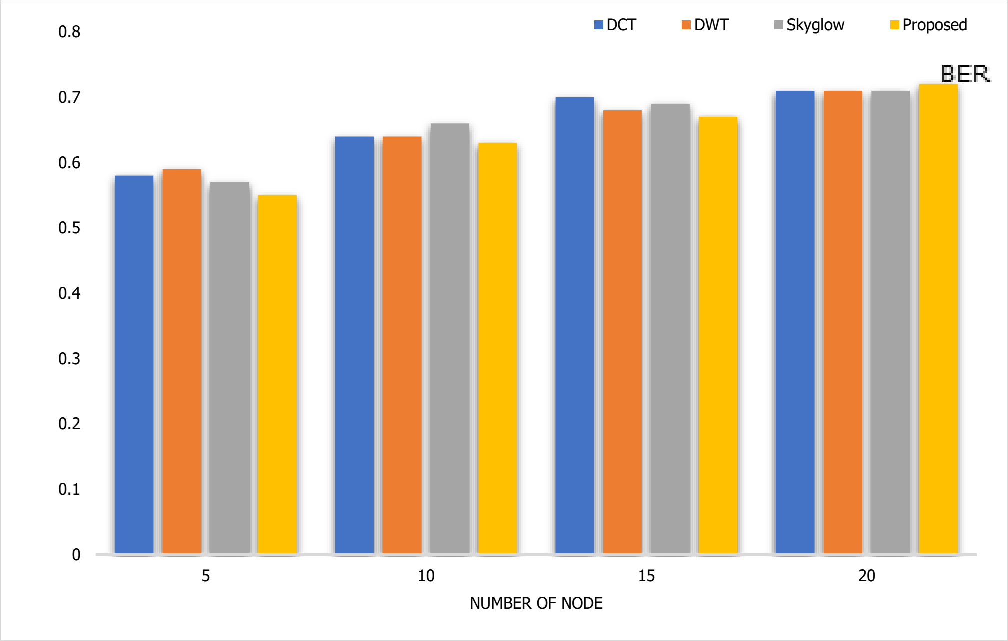

Figure 6: Comparative performance of different techniques for BER with number of node5, 10, 15, 20.

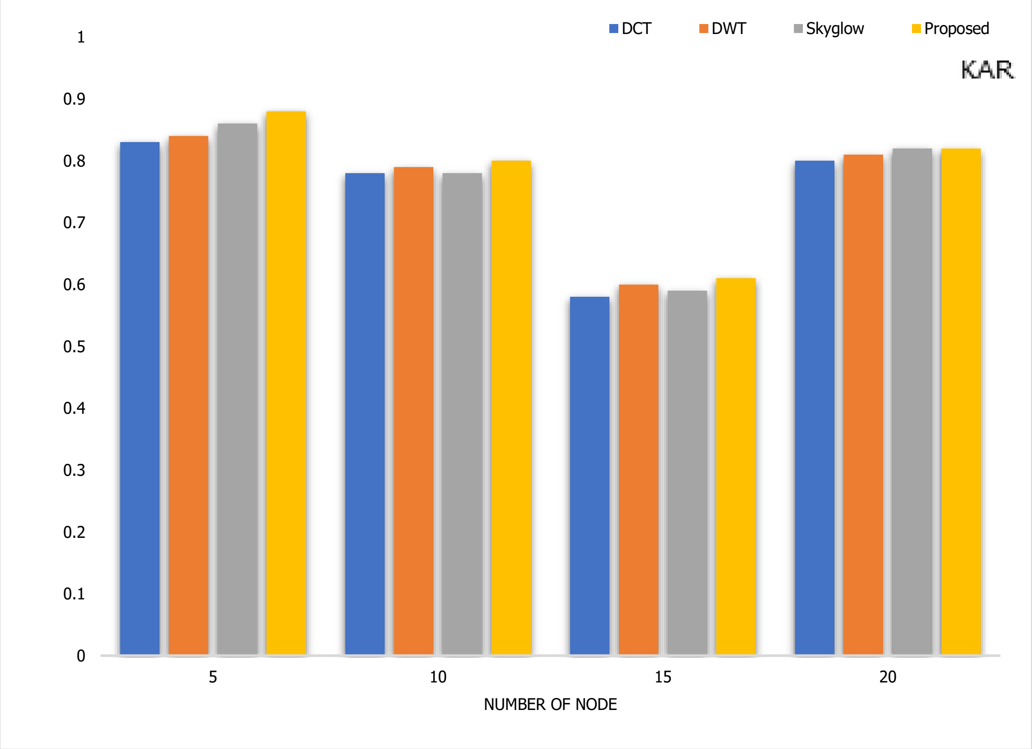

Figure 7: Comparative performance of different techniques for KAR with number of node 5, 10, 15, 20.

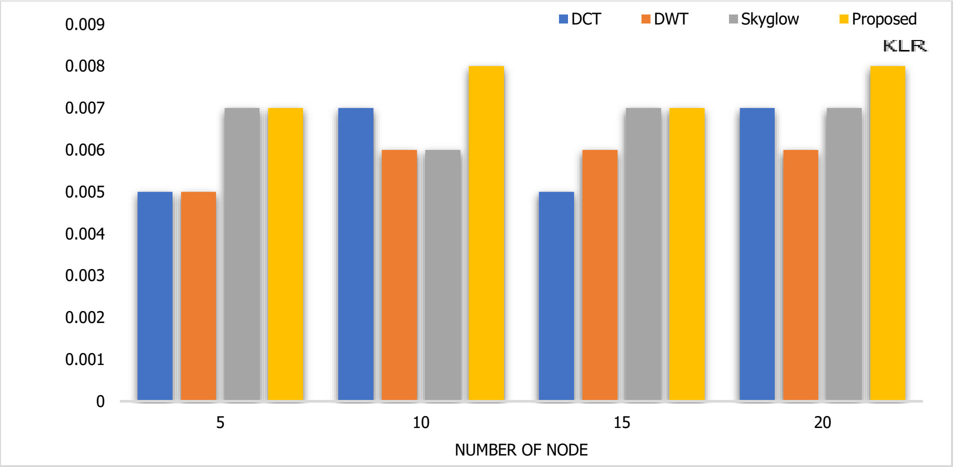

Figure 8: Comparative performance of different techniques for KLR with number of node5, 10, 15, 20.

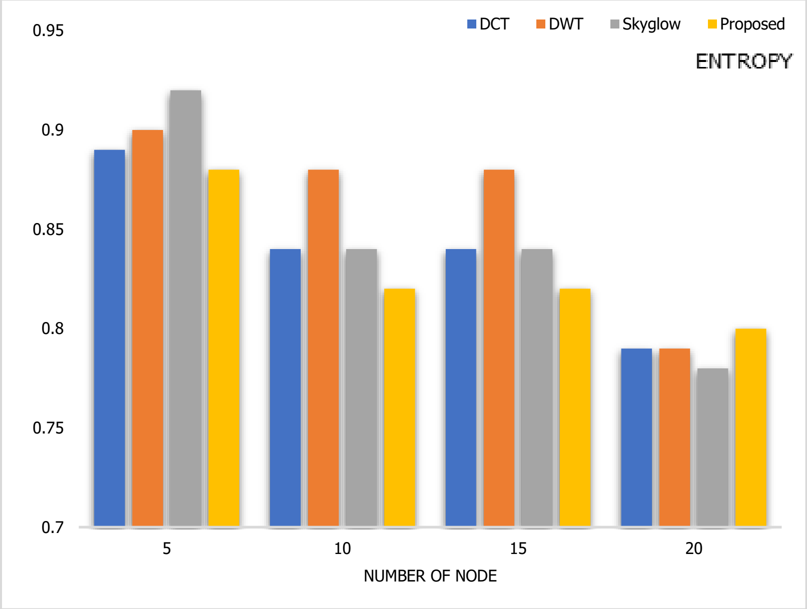

Figure 9: Comparative performance of different techniques for entropy with number of node5, 10, 15, 20.

CONCLUSION

This paper proposes the DCT based system as an efficient key generation system and synchronized quantization (SQ) as a part of the key generation system that synchronizes data blocks in the quantization phase in order to eliminate the signal pre-processing and error-correcting phase. The efficiency of the system is indicated by lower computing time and the communication overhead between authorized nodes compared to existing systems. Validation of the proposed system performance is carried out in two real indoor environment scenarios, i.e., unobstructed and the obstacles scenarios. The test results showed that the proposed method was able to produce equal 128-bit keys without going through the signal pre-processing and error-correcting phase with KAR values reaching 1.05 bps. Testing of computing time and the communication overhead in two scenarios also show the efficiency of the proposed system compared to the existing system.

REFERENCES

[1] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper." *Digital Communications and Networks* 4, no. 3 (2018): 149-160.

[2] Tang, Shu, Dennis R. Shelden, Charles M. Eastman, Pardis Pishdad-Bozorgi, and Xinghua Gao. "A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends." *Automation in Construction* 101 (2019): 127-139.

[3] Chettri, Lalit, and Rabindranath Bera. "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems." *IEEE Internet of Things Journal* 7, no. 1 (2019): 16-32.

[4] Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." *Telecommunication Systems* 67, no. 3 (2018): 423-441.

[5] Allhoff, Fritz, and Adam Henschke. "The internet of things: Foundational ethical issues." *Internet of Things* 1 (2018): 55-66.

[6] Aly, Mohab, Foutse Khomh, Mohamed Haoues, Alejandro Quintero, and Soumaya Yacout. "Enforcing security in Internet of Things frameworks: A systematic literature review." *Internet of Things* 6 (2019): 100050.

[7] Ahmad, Mudassar, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, and Syed Hassan Ahmed. "A review of current security issues in Internet of Things." In *Recent Trends and Advances in Wireless and IoT-enabled Networks*, pp. 11-23. Springer, Cham, 2019.

[8] Bedi, Guneet, Ganesh Kumar Venayagamoorthy, Rajendra Singh, Richard R. Brooks, and Kuang-Ching Wang. "Review of Internet of Things (IoT) in electric power and energy systems." *IEEE Internet of Things Journal* 5, no. 2 (2018): 847-870.

[9] Bhattacharjya, Aniruddha, Xiaofeng Zhong, Jing Wang, and Xing Li. "Security challenges and concerns of Internet of Things (IoT)." In *Cyber-Physical Systems: Architecture, Security and Application*, pp. 153-185. Springer, Cham, 2019.

[10] Bhattarai, Sulabh, and Yong Wang. "End-to-end trust and security for Internet of Things applications." *Computer* 51, no. 4 (2018): 20-27.

[11] Bhattacharjya, Aniruddha, Xiaofeng Zhong, Jing Wang, and Xing Li. "Present Scenarios of IoT Projects with Security Aspects Focused." In *Digital Twin Technologies and Smart Cities*, pp. 95-122. Springer, Cham, 2020.

[12] Shah, Nirali, Chintan Bhatt, and Divyesh Patel. "IoT gateway for smart devices." In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, pp. 179-198. Springer, Cham, 2018.

[13] Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. "The industrial internet of things (IIoT): An analysis framework." *Computers in industry* 101 (2018): 1-12.

[14] Chae, Bongsug Kevin. "The evolution of the Internet of Things (IoT): A computational text analysis." *Telecommunications Policy* 43, no. 10 (2019): 101848.

[15] Chifor, Bogdan-Cosmin, Ion Bica, Victor-Valeriu Patriciu, and Florin Pop. "A security authorization scheme for smart home Internet of Things devices." *Future Generation Computer Systems* 86 (2018): 740-749.

[16] da Costa, Kelton AP, João P. Papa, Celso O. Lisboa, Roberto Munoz, and Victor Hugo C. de Albuquerque. "Internet of Things: A survey on machine learning-based intrusion detection approaches." *Computer Networks* 151 (2019): 147-157.

[17] Di Martino, Beniamino, Massimiliano Rak, Massimo Ficco, Antonio Esposito, Salvatore Augusto Maisto, and Stefania Nacchia. "Internet of things reference architectures, security and interoperability: A survey." *Internet of Things* 1 (2018): 99-112.

[18] Ekanayake, Binara NB, Malka N. Halgamuge, and Ali Syed. "Security and privacy issues of fog Computing for the internet of things (IoT)." In *Cognitive Computing for Big Data Systems Over IoT*, pp. 139-174. Springer, Cham, 2018.

[19] Elrawy, Mohamed Faisal, Ali Ismail Awad, and Hesham FA Hamed. "Intrusion detection systems for IoT-based smart environments: a survey." *Journal of Cloud Computing* 7, no. 1 (2018): 21.

[20] Gupta, B. B., and Megha Quamara. "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols." *Concurrency and Computation: Practice and Experience* (2018): e4946.