Proceedings

Of the

12th International Multi-Conference on ICT Applications

Theme:

APPLICATION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY TO TEACHING, RESEARCH AND ADMINISTRATION

AICTTRA 2018

Venue

MAIN AUDITORIUM
AFRICAN CENTRE OF EXCELLENCE
(OAK-Park)
OBAFEMI AWOLOWO UNIVERSITY
ILE-IFE, NIGERIA.

OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE.
Department of Computer Science and Engineering
In collaboration with
Africa Centre of Excellence:
OAUICT Driven Knowledge Park

ISSN 2141 - 0240

The 12th International Multi-Conference on ICT Applications

With the Theme

Application of
Information and Communications Technology
To Teaching, Research and Administration

AICTTRA 2018

November 11th – 14th, 2018

@

Main Auditorium
African Centre of Excellence *(OAK-Park)*
Obafemi Awolowo University, Ile-Ife, Nigeria

PROCEEDINGS

Volume XII

Edited by

Professor E.R. Adagunodo
Professor G.A. Aderounmu
Dr. A. I Oluwaranti
Dr. E.A. Olajubu
Dr. B.I. Akhigbe
Dr. I.P. Gambo

Organized by
Department of Computer Science & Engineering
In Collaboration with
African Centre of Excellence: OAUICT Driven Knowledge Park
Obafemi Awolowo University

FOREWARD

It is my great pleasure and delight to welcome all of us to the 12th International Conference on Application of Information and Communication Technology to Teaching, Research and Administration tagged AICTTRA 2018, which is holding at the African Centre of Excellence (OAK-Park), Obafemi Awolowo University, Ile-Ife, Nigeria between November 11th and 14th, 2018. I understand that conferees came from different places and beyond to attend this great event. I usually refer to the conference as a pilgrimage for ICT professionals and enthusiast. A total of 45 well written and reviewed papers have been selected for presentation at different times in the conference.

The Programme of the conference is a varied one that reveals the wide range of application to which ICT is being put and exposes the impossibility of placing any specific bounds or limits on the field. The field of ICT has continued to grow with mind blowing evidences in its area of application. To be able to compare note and learn from each other through the exploration of techniques remain the motivation to hold this conference year in year out. Thus, this quest has been on as a matter of strict business as was in the previous eleven versions of the conference. This twelfth edition seeks a multi-conference approach to the forgoing, and promises to extend the frontiers of the exploration of the deployment of ICT in various spheres of human activities.

The programme of the conference has been threaded into parallel sessions. The sessions promised to stimulate fruitful debate on emerging areas of research in the use of ICT. We are sure that cutting edge issues have been included in organized syndicate and informal discussion sessions that will take place during the conference. This promises to be useful and informative.

The President, Nigeria computing Society (NCS), Professor G.A. Aderounmu, and the current Dean of the Faculty of Technology, Obafemi Awolowo University happens to be one of the initiators of the conference will be on hand to share his wealth of experiences in teaching, research and administration. There will be lead paper presentations by eminent researchers and practitioners in ICT. The organizers of the event owe special thanks to the Vice-Chancellor of Obafemi Awolowo University, IIe-Ife, Nigeria, Professor E.O. Ogunbodede for his continuous support in the organization of the conference.

We are also very grateful to one of the fathers of this conference - Professor L.O. Kehinde, for his support. To the Chairman LOC - Dr. A.I. Oluwaranti and his technical team and members such as Dr. E.A. Olajubu (Vice Chair LOC), Dr. B.O. Akinyemi, Dr. B.I. Akhigbe, Dr. I.P. Gambo, Dr. S.A. Bello, Dr. R.N. Ikono, Dr. S. Aina, Dr. H.O. Odukoya, Engr. Tope Ajayi, Ms. A.R. Lawal who had all worked tirelessly to ensure the success of this conference; I say a big thank you and congratulations for a job well done. I also appreciate the members of staff - academic, non-academic, and technical - for their immense support towards the conference. This conference could not have been successful without the support of individuals and several corporate entities, which time will not permit to mention. All the same, our thanks go to all of them for their continuous belief in the conference and continual support. You are all wonderful people and great as well, and most especially all the attendees in this year’s Conference.

Professor E. R. Adagunodo
Department of Computer Science & Engineering,
Obafemi Awolowo University, Ile-Ife, Nigeria.

LIST OF REVIEWERS

S/No	Name of Reviewers	Contact Address
1.	Prof. E.R. Adagunodo	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
2.	Prof. G.A. Aderounmu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
3.	Prof. K. Gbolagade	Kwara State University, Ilorin, Kwara State
4.	Dr. A.O. Oluwatope	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
5.	Dr. B.S. Afolabi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
6.	Dr. (Mrs.) R.N. Ikono	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
7.	Dr. K.I. Ogundoyin	Department of Computer Science, Osun State University, Osogbo
8.	Dr. S.A. Akinboro	Department of Computer Science, Bells University, Otta, Ogun State
9.	Dr. C.O. Akanbi	Department of Computer Science, Osun State University, Osogbo
10.	Dr. L.A. Akanbi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
11.	Dr. A.O. Ajayi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
12.	Dr. A.A. Adeyelu	Department of Mathematics & Computer Science, Benue State University, Makurdi
13.	Dr. P.A. Idowu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
14.	Dr. (Mrs.) A.R. Iyanda	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
15.	Dr. (Mrs.) B.O. Akinyemi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
16.	Dr. A.I. Oluwaranti	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
17.	Dr. (Mrs.) G.O. Binuyo	African Institute for Science Policy and Innovation, Obafemi Awolowo University, Ile-Ife.
18.	Dr. F.O. Asahiah	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
19.	Dr. (Mrs.) S.A. Bello	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
21.	Dr. S. Aina	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
22.	Dr. O. Osunade	Director, Information Technology and Media Services, University of Ibadan, Ibadan

S/No.	Name of Reviewers	Contact Address
23.	Dr. O.F.W. Onifade	Department of Computer Science, University of Ibadan, Ibadan
24.	Dr. (Mrs.) M.L. Sanni	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
25.	Dr. H.O. Odukoya	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
26.	Dr. O.A. Ojesanmi	Department of Computer Science, Federal University of Agriculture, Abeokuta
27.	Dr. A.O. Akinwumi	Department of Computer Science & Information Technology, Bowen University, Iwo
28.	Dr. A.S. Sodiya	Department of Computer Science, Federal University of Agriculture, Abeokuta
29.	Dr. S.A. Onashoga	Department of Computer Science, Federal University of Agriculture, Abeokuta
30.	Prof. S. Tanko	University of Jos, Nigeria & Scarborough, North Yorkshire, United Kingdom
31.	Dr. O.O. Abiona	Department of Computer Information Systems, Indiana University, North West U.S.
32.	Dr. Jimoh	Department of Computer Science, University of Ilorin, Ilorin
33.	Dr. (Mrs.) I.O. Awoyelu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
34.	Dr. (Mrs.) O.D. Ninan	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
35.	Dr. R.G. Jimoh	Department of Computer Science, University of Ilorin, Kwara State.
36.	Dr. S.I. Eludiora	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife

ENTROPY MANAGEMENT TECHNIQUE IN LIGHTWEIGHT CRYPTOGRAPHICALLY SECURED SMART HOME

*[1]Oluwade O. R., [2]Olaniyi O. M., [2]Abdulsalam Y. S. & [2]Ajao L.A.
[1]Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
[2]Department of Computer Engineering, Federal University of Technology, Minna, Niger-state, Nigeria.

*E-mail: oluwade.pg717576@st.futminna.edu.ng

ABSTRACT

The proliferation of Internet of Things (IoT) and its applications have affected every aspect of human endeavours; from smart manufacturing, agriculture, healthcare, logistics, Government, cities, transportation to Homes. The ubiquitous nature of IoT makes the security of information on transit and at rest a great concern, especially to smart home appliances. Non-computer and non-smartphone nature of IoT devices such as alarms, internet-connected "wearable" devices, thermostats and refrigerators make the devices, environment and users vulnerable to malicious attacks. This comes as a result of lack of built-in security facilities for IoT and smart home devices. Also, this has brought about security and privacy challenges as regards confidentiality, integrity and authentication. In this paper, we present entropy management through entropy shifting, stretching and mixing techniques to enhance the traditional Tiny Encryption Algorithm (TEA). The technique is developed to address "equivalent keys" in information encryption and device security of appliances in smart homes. This work provides security for smart homes through entropy management technique that overcomes the weakness of "equivalent keys" and the unique "small footprint" in the traditional TEA.

Keywords: Internet of Things, Lightweight Cryptography, Smart home, Tiny Encryption Algorithm.

1.0 INTRODUCTION

Internet of Things (IoT) in recent years with its potentials has positively affected every aspects of human endeavors, ranging from manufacturing, agriculture, healthcare, businesses, logistics, Government, cities and homes [1]. The term "Internet of Things" generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human intervention [2].

A smart home is one of the areas of applications of IoT [3]. Smart home is a network of connected devices in human living environment, which communicate remotely or in automation with each other and the inhabitants to raise their living and quality of life, the efficiency of energy consumed and their safety [4].

The ubiquitous nature of IoT is partly as a result of its usage of the existing technologies such as Wireless Sensor Networks, Radio Frequency Identification (RFID) and cloud computing which serve as ready-platform for its communication.

Traditional cryptographic security measures cannot be applied to the low-capacity devices known as constrained IoT devices. Flexible security infrastructure is hence needed for the IoT such as Lightweight Cryptography [5]. Lightweight cryptography is a cryptographic algorithm or protocol that is designed to function in constrained devices known as smart devices or environment such as sensors, health-care devices, RFID tags, and contact-less smart cards.

Cryptography is a basic important technique for securing data at rest in storage devices or in transit. This was achievable in the past by keeping secret, the cryptography algorithms and codes, but recently securing cryptography depends largely on having strong keys and keeping them secret [6]. The strength of a cryptographic key depends on the degree of how hard it is to guess. The degree of hardness of a key depends on the degree of randomness used in generating the key [6].

Generating random numbers is essential to cryptography, and generating true random information is the most crucial of cryptographic algorithm to effectively aid in security key management [7]. Entropy is a measure of randomness or uncertainty in a signal and the sufficiency of it, the better in key generation [6].

This work addresses issues of vulnerability attacks such as malicious nodes attack, man-in-the-middle attack, privacy and key related attacks in Smart home using a lightweight TEA entropy management for securing smart homes and appliances. In addressing the issues of vulnerability attacks on smart home and appliances, an enhanced TEA would be developed, through entropy management technique to proffer solution to related key attacks.

The organization of this paper is as follows: Section 1 introduces smart home based internet of things technology and secure entropy management cryptography techniques.

Section 2 reviews related literature and works on lightweight cryptography and key management as related to smart devices. Section 3 highlights the methodology used in the research, while Section 4 and 5 give result and conclusion respectively.

2.0 LITERATURE REVIEW

2.1 Internet of Things, smart home and Threats

The ubiquitous nature of IoT, the non-computer and non-smartphone nature of its devices such as refrigerators, thermostats, and internet-connected “wearable” devices make the security of information on transit and at rest a great concern [8]. Users of the smart devices are also vulnerable to malicious attacks. IoT and smart home devices were not designed with built-in security facilities, which bring about security and privacy challenges as regards confidentiality, integrity and authentication. Smart home is application of Internet of Things and hence this is a home or living environment where home appliances/devices are able to interact automatically and be able to be controlled remotely [3].

igure 1 shows the architecture of a smart home. Smart home architecture includes a gateway/server/router as a connection within the home and then to the smart home appliance(s). Some of the communication methods or topologies used in Home Area Network (HAN) are: Z-Wave, Zigbee, Powerline, Bluetooth [9].

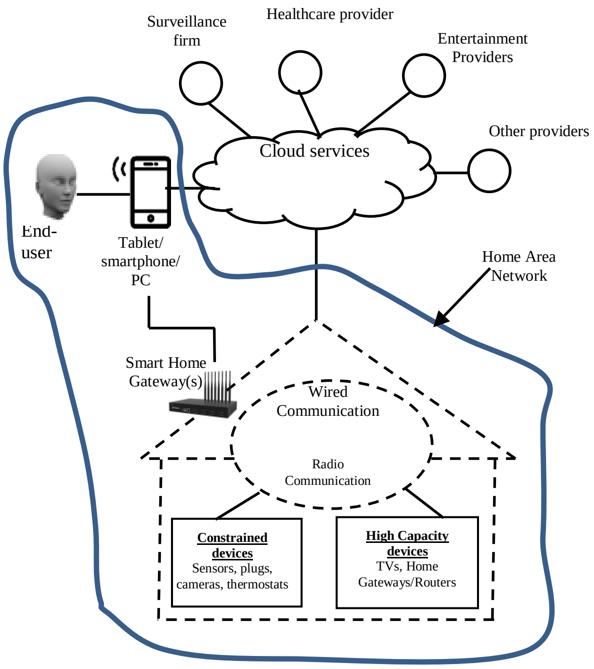

Figure 1: Architecture of a typical smart home (Adapted from Gabriele, *et al.* 2016)

Any or a combination of these available external networks such as digital subscriber lines (xDSL), phone line and cable can be used to complete the installation [10]. Figure 2 shows the Home Area Network (HAN) in a smart connected Home Architecture.

Practically the smart home is simply putting a computer in one’s home, connected to a home router and every other imaginable appliances and devices are connected to it [4]. Afterwards, one is able to control it with either a web browser or a smartphone. “Kitchen Computer” by Neiman Marcus was one of the first smart home devices [11]. From the report of Cisco’s Internet Business Solution Group, IoT really came into existence between 2008 and 2009 due to the introduction of ubiquitous smart devices in the likes of smart phones in 2007 [12].

Today, the number of connected smart devices is alarming and there is prediction that by 2020, there would be 50 billion smart devices connected to the internet, almost doubling the present connected smart devices [12]. According to [13], areas of application of smart home are: home appliances, home utility systems and home safety and security systems.

[4] puts the areas of applications to be: light control/automation, entertainment, alarm system, intelligent white goods which comprises of appliances that automatically carry out actions like fridge automatically ordering missing items. Others are *Heating, ventilation, and air conditioning* (HVAC)*)* systems and assisted living to aid or assist the invalid, the aged or physically challenged through automation of different tasks and monitoring of vital indices.

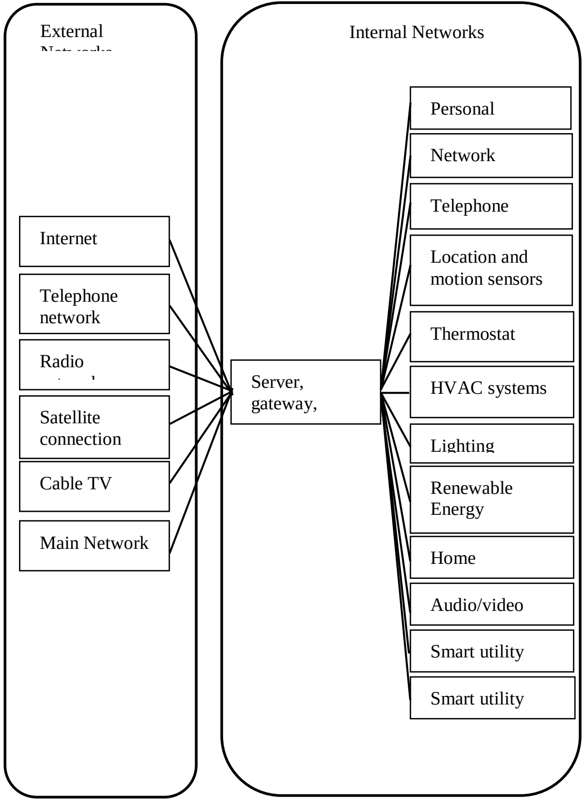

Figure 2: Home Area Network in smart Connected Home Architecture (Joseph, *et al.* 2016)

The smart home system has very huge positive impacts on human daily lives and thus there are associated threats with it. The associated threats are on “life and health”, information, property and control of access to connected devices and home [4]. “Life and health” has the widest spectrum of threats and ranges from eavesdropping to serious fatal hacking [11]. The rate at which home network is growing, overwhelmingly comparable to small offices, management and security of the connected devices have become important issues for consideration by both the producers and users of the connected smart appliances [14], because large, important and confidential data and information are shared among devices and users, so security and privacy of IoT is very complicated compared to other networks. Areas of security concerns in IoT are: confidentiality, integrity, authentication and authorization [15].

Few examples showing the impacts of ineffective security on constrained devices are: firstly, Dick Cheney, a former Vice President of US whose pacemaker's wireless capability had to be disabled due to the concerns that his heart could receive fatal shock from hackers [16]. Secondly, a German government agency issued a warning on a talking doll that its smart technology could reveal personal data due to an unsecure Bluetooth device and that hackers could listen and talk to a child playing with the doll [17]. Thirdly hackers could break into ones Electric meter, remotely reading the meter or shutting down power supply to a house [18].

Security solutions for IoT (and smart home) are still vulnerable to attacks such as: man in the middle, masquerading, eavesdropping, saturation, Denial of Service (DoS) and key related attacks [15].

According to [15], cryptography algorithm can be used to solve the security challenge in IoT to maintain the trust of users. Standard traditional heavy weight algorithms are too energy consuming, too big or too slow for constrained devices [19]. Lightweight cryptography – either symmetric or asymmetric could bring about the needed solution to the security challenge [15].

2.2 Lightweight Cryptography

Cryptography is the science of secret writing which is an ancient art dated back as far as 1900 B.C. being used by Egyptian scribes, though some experts argue that cryptography came to be, the same time writing was invented [20]. Also, cryptography is mathematical algorithms used in encrypting and decrypting messages, but the advent of computer communication brought about new form of cryptography in telecommunication and data communication over the internet or untrusted medium [20].

The five primary functions of cryptography are: i.) Authentication – Proving of one's identity; ii.)Integrity – Giving assurance to recipient of message that the message received him has not been tampered, hence assurance of originality; iii.) Key exchange – This is a way of exchange or sharing of crypto keys between the sender and the receiver. iv.) Privacy/Confidentiality – This is ensuring no body reads the message except the receiver whom it was meant for v.)Non-repudiation – This is a means of proving that the sender actually sent the message.

Cryptographic algorithms can be categorized in several ways. But in this paper, categorization would be done based on the number of keys used in encryption and decryption. Based on this, three types of cryptographic algorithms [20] are discussed. Figure 3 shows types of cryptography based on the number of keys for encryption and decryption.

(i) **Secret Key Cryptography (SKC) – In this cryptography, a** *single key is used for both the encryption* and decryption processes. This is also known as symmetric encryption. Essentially this is used for confidentiality and privacy. The greatest challenge in this form of cryptography is the distribution of the key between the sender and recipient of the information. This cryptography is generally categorized as either block ciphers or stream ciphers (cypher could also be said to mean encryption algorithm). Example of SKC are: Data Encryption Standard, Advance Encryption Standard (successor to DES), CAST 128/256, International Data Encryption Algorithm (IDEA), Rivest Ciphers, Blowfish, Twofish, Camellia, Kasumi, SEED, ARIA, Skipjack, Tiny Encryption Algorithm (TEA) and CLEFIA to mention but a few.

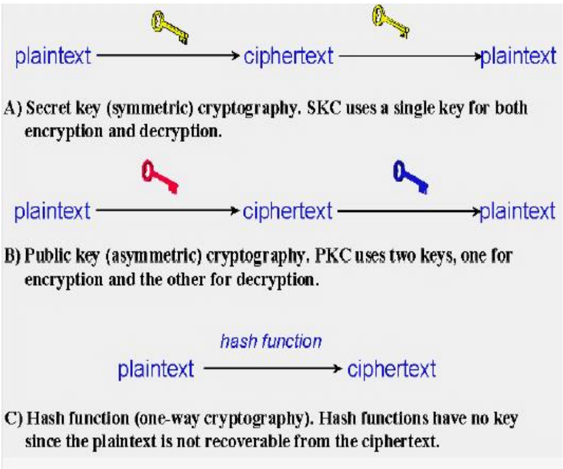
plaintext
ciphertext
plaintext
A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.
plaintext
ciphertext
plaintext
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.
hash function
plaintext
ciphertext
C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 3: Types of Cryptography: Secret Key, Public key, and Hash function. (Gary C. K. (2018).)

(ii) Public Key Cryptography (PKC) – This utilizes two different keys, which are one for encryption and the other decryption. One of the keys is set as the public key and can be advertised far and wide, while the other is set as the private key and never revealed to anybody. This is essentially used for key exchange, non-repudiation and authentication. Examples of PKC are: Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA), named after the three MIT mathematicians who developed it, Diffie-Hellman (D-H), Digital Signature Algorithm (DSA), ElGamal, and Elliptic Curve Cryptography (ECC).

(iii) Hash Functions – This is also known as one way encryption or message digests. This algorithm does not use key, but fixed-length hash value that is computed from the plaintext, and thus making it difficult to discover the length and content of the plaintext. This irreversibly encrypts a message using mathematical transformations and providing a digital fingerprint. One cannot take a hash and decrypt it to recover the content that originally created it. This algorithm is essentially used for message integrity. Examples of Hash algorithms in use are: Message Digest (MD) algorithms, (which are series of byte-oriented algorithms producing 128 bits hash values from messages of arbitrary lengths, such as MD2, MD4, MD5), Secure Hash Algorithm (SHA) (in the variants of SHA-1, SHA-2, SHA-3, SHA-224, SHA-256, SHA-386, and SHA 512), RIPEMD, HAVAL, Whirlpool and Tiger.

Lightweight cryptography is usually referred to as cryptography for resource-constrained devices. By lightweight, we do not mean that it is less secured, but the devices needing security are resource constrained and the hackers are not. Hence we need security techniques that are lightweight in resource constrained devices [21]. Lightweight cryptography has the ability of effecting secure encryption on constrained devices and environments such as sensors, RFID tags, and healthcare devices with limited resources [22].

Lightweight cryptography is a researched technology that is developed to effect security on data or information on transit or at rest through encryption. It serves as countermeasure to attacks on data and information [22]. Lightweight cryptography is a cryptographic protocol or algorithm that is used on constrained devices, and is required for IoT because of these reasons: Firstly, the low resource-devices are battery-powered devices, with limited amount of energy consumption. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices. Secondly, the footprint of the lightweight cryptographic primitives is smaller than those of the conventional algorithms'. The lightweight cryptographic algorithms enable connections with lower resource devices. Table 1 shows comparisons of some lightweight cryptography algorithms used in IoT. Tiny Encryption Algorithm (TEA) is used for this research because of its small size, code length, rich key size and moderate block size and its Feistel structure [23].

Table 1: Comparison of Symmetric Lightweight Algorithms in IoT

S/No.	Symmetric Algorithm	Structure	Number of rounds	Key size K	Block size	Possible Attacks	Source Literature
1	AES	SPN	10	128	128	Man-in-middle attack	[15]
2	Hight	GFS	32	128	64	Saturation Attack	[15]
3	TEA	Feistel	32	128	64	Related Key Attack	[15]
4	PRESENT	SPN	32	80	64	Differential Attack	[15]
5	RC5	ARX	20	16	32	Differential Attack	[15]
6	CAST-128	Feistel	12 or 16 16 when K>80	40-128	64	Differential Attack	[15], [24]
7	CAST-256	Feistel	14	256	128	Differential Attack	[15], [24]
8	Blowfish	Feistel	16	32-448	64	Differential Attack	[15], [24]
9	Twofish	Feistel	16	128, 192, 256	128	Related Key Attack	[32]
10	IDEA	Substitution - Permutation	8	128	64	Related key Attack	[32]
11	DES	Feistel	16	64	64	Brute Force, Related Key	[32]
12	BLOWFISH	Feistel	16	128-448	64	Related key Attack	[32]

2.3 Tiny Encryption Algorithm (TEA)

Tiny Encryption Algorithm (TEA) is a small algorithm, simple, fast and strong cryptographically. TEA was originally designed by Wheeler and Needham [26]. TEA is block cipher, known for its simplicity in codes of few lines and implementation.

The design of TEA to be a very small (tiny) algorithm with short software codes and small footprint as regards its memory occupation when stored, made it seamlessly fit into any program on any computer. This was achieved by making simple and weak, its basic operations [27].

Security challenges are overcome by repeating the basic operations repeatedly [27]. A credit to TEA is its high speed in encryption processes, but notable drawbacks of TEA are its use of "equivalent keys" which weakens its key length effectiveness and only requires complexity O(2ˆ32) which is even much lesser than the effort 2ˆ128 required for brute force attack to break the key. The other notable drawback is that there is no known standard to which TEA is measured as regard the codes' length [27].

TEA is Feistel cipher whose operation utilises mixed algebraic groups, which are XOR, ADD and SHIFT. This operation really utilises the twin properties of Shannon – diffusion and confusion which are important for block cipher. TEA encrypts 64bits data at a time by using 128-bit key and its highly resistant to differential attacks. Related key attacks are possible with TEA, though its mixing portion seems to be okay [26].

This research aims to correct this observed weakness in TEA, through entropy management. TEA is a lightweight algorithm that suits smart home cryptographic processes. Figure 4 shows A Single Round TEA – Comprising 2 Feistel Operations.

TEA's specification is that 32 rounds of TEA be completed for every encrypted 64-bit block. ***Diffusion*** works to hide any statistical information between the plaintext and the ciphertext that may serve as backdoor to the attackers, while ***confusion*** ensures that the statistical information between the ciphertext and the encryption key are kept secured, to thwart any effort of the attackers discovering the key [28].

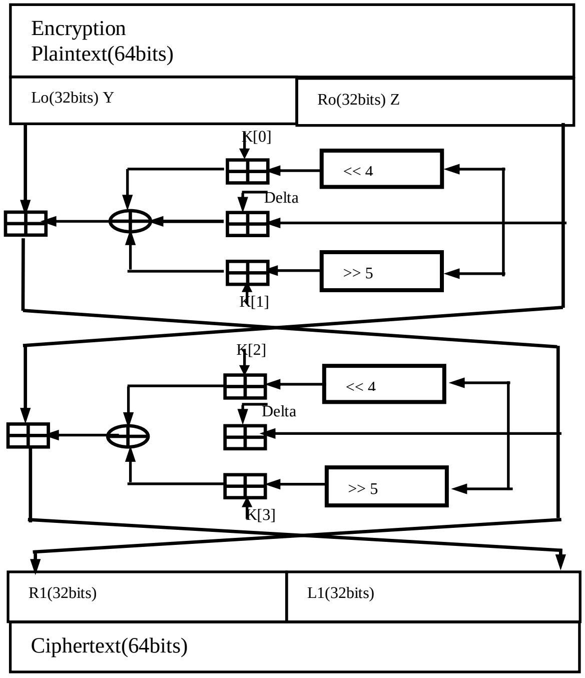

Figure 4: A Single Round TEA – Comprising 2 Feistel Operations

Diffusion and confusion are achieved in Feistel Cipher Structure as illustrated in Figure 4 through the use of substitution and permutation. ***Substitution*** (addition, XOR'ing and shifting) operation is performed on the left (L) of the plaintext, while ***permutation*** operation is swapping at every round, of both halves of the plaintext.

Many symmetric block ciphers, such as Tiny Encryption Algorithm and Data Encryption Standard made use of Feistel cipher structure. By specification, TEA has a 128-bit key which is divided into four, to give 32-bits key word length (K0, K1, K2, K3 as in Figure 4) that work on a 64-bit data block that is split into two 32-bit blocks called L and R (left and Right side of the data block).

The operations in the first half of the first round of TEA as in Figure 4 are: 1.) R has a left shift of 4 and then added to K0, 2.) R added to Delta $[(\sqrt{5}-1)*2^{31}]$. R passes through a right shift 5 and added to K[1]. The three operations had XOR operation applied to their result. The result obtained now serves as R for the next Feistel round because at this time, swap is carried out on R and L

2.4 Entropy

The key K for use in TEA would have to be generated. Availability of good entropy is a necessity for generating unpredictable keys [29], and best algorithm cannot compensate for generation of weak keys using insufficient entropy [6]. Hence if an encryption key to any smart appliance is predictable, then the appliance is vulnerable to malicious attack. There are so many instances where random numbers are needed such as: simulation of randomness in Monte Carlo method, protocols, online gambling, Nonce generation and key generation (session key, main key) [30].

Entropy is a major player in cryptography, whose intent is to enable communication to take place securely between two nodes not minding the adversaries [4]. Entropy is a measure of randomness or uncertainty in an output of data sources. This was first introduced by C. E. Shannon as a center point of his work in 1948. Entropy is the most common term used when describing random number generators (RNG) [31].

A random number generator is an algorithm that uses an initial seed or a continuous input to produce a sequence of numbers or bits [31]. One of the areas of difficulties in cryptographic algorithms is in the area of generating true random numbers to use for the cryptographic key(s) [6].

Generally there are two kinds of random numbers generators, which are: non-deterministic random number generators, known as "True Random Number Generators" (TRNG) and deterministic random numbers generators, also called: "Pseudo Random Number Generators (PRNG) [31]. True random number generators are obtained from chaotic physical processes, like atmospheric noise and thermal noise, but have low bit rate and cannot measure up to the requirements or needs of most cryptosystems [32].

Another source of entropy from computer is grouped into hardware and software which are deterministic and are known as PRNGs. Examples of hardware entropy sources are chips with built-in ring oscillators [32], noisy diodes, techniques for using flash memory and human driven movement of mouse and keyboard stroke timings [6]. Software as source of entropy can run as stand-alone or be directly incorporated into software applications [6]. Because of the inability of TRNGs to produce quality and quantity entropy to satisfy the needs of the cryptosystems, PRNG with its speed of entropy generation is a welcome development in entropy generation, even as a service [33]. In this research, PRNG is used in entropy generation for key management in smart home constrained appliances.

3.0 METHODOLOGY

3.1 Architecture and Technique

This section explains the architecture and algorithm for the secure smart home appliances using lightweight TEA entropy management. Figure 5, shows the developed system architecture

In the design flowchart shown in figure 6, the first round of random number generation of pool 1(Java) and pool 2(C++) are added together placed in C_1, while the second round of random number generation of pool 1 and pool 2 are added together and placed in C_2.

This is shifting technique. $C_1$and $C_2$are then concatenated to achieve entropy stretching technique, and result placed in D1. Round 1 and round 2 are repeated and the final result placed in D2. Entropy mixing is achieved by D1 been XORed with D2. The resultant entropy H, (D.D) is the key K to be used on TEA.

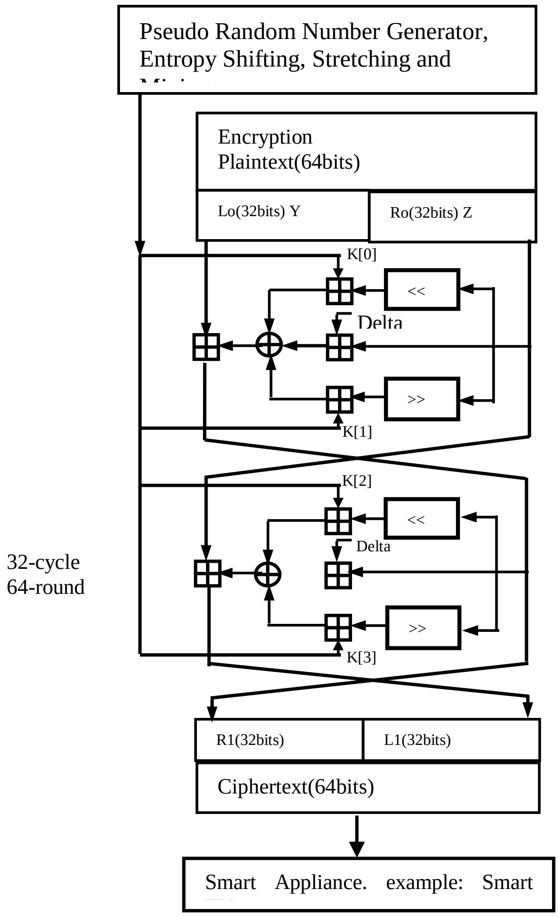
Pseudo Random Number Generator, Entropy Shifting, Stretching and
Encryption Plaintext(64bits)
Lo(32bits) Y
Ro(32bits) Z
K[0]
<<
Delta
>>
K[1]
K[2]
<<
Delta
32-cycle 64-round
>>
K[3]
R1(32bits)
L1(32bits)
Ciphertext(64bits)
Smart Appliance. example: Smart

Figure 5: The Developed System Architecture

3.2 Modula Steps

Entropy is generated using the random number generation function in C++ and Java programming languages and seeded with the system's time function. There are three steps involved in the whole entropy management before usage with TEA. The steps are: Entropy-shifting, Entropy-stretching and Entropy-mixing. The essence of utilising two programming languages is to make the final entropy (key) undecipherable by the hackers.

Entropy *H*, is mathematically expressed as:

$$H = \log_2 (b^l) \qquad 1$$

Where *b* is the number of possible symbols and *l* is the number of symbols in the password [34].

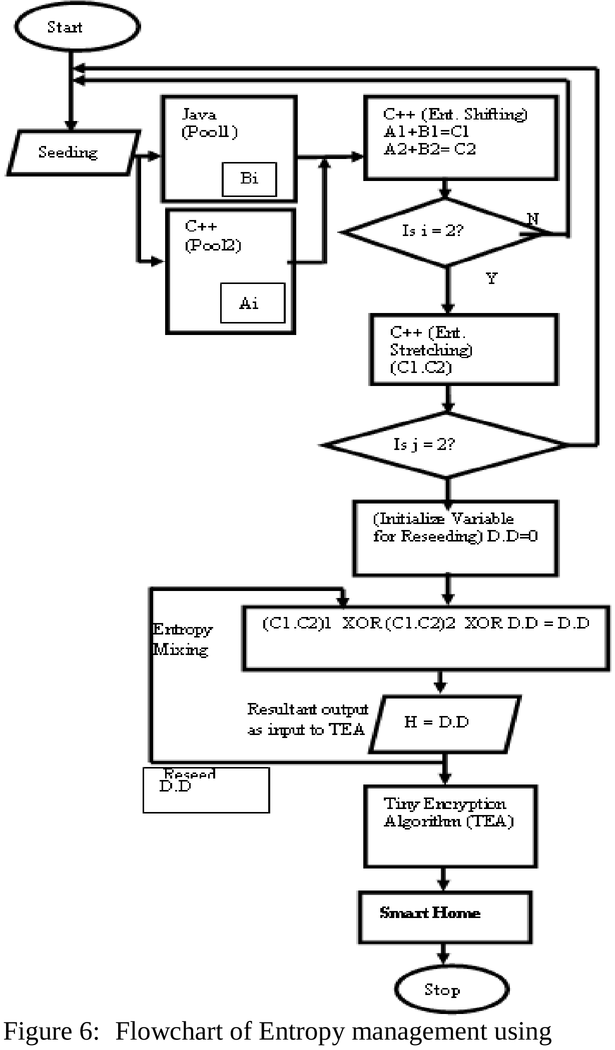
Start
Seeding
Java (Pool1)
Bi
C++ (Pool2)
Ai
C++ (Ent. Shifting) A1+B1=C1 A2+B2= C2
Is i = 2?
N
Y
C++ (Ent. Stretching) (C1.C2)
Is j = 2?
(Initialize Variable for Reseeding) D.D=0
Entropy Mixing
(C1.C2)1 XOR(C1.C2)2 XOR D.D = D.D
Resultant output as input to TEA
H = D.D
Reseed D.D
Tiny Encryption Algorithm (TEA)
Smart Home
Stop

Figure 6: Flowchart of Entropy management using Entropy Shifting, Stretching and Mixing

Module 1 - Entropy Shifting

The theory behind entropy shifting is the movement of entropy from a pool 1 (storage 1) of entropy to another pool 2 (storage 2) of entropy (Andrea, 2005).This movement causes depletion of entropy in pool 1 and increment of entropy in pool 2. Java written codes serve as pool 1, while codes in C++ serve as pool 2. Entropy is generated using the random number generation function in C++ seeded with the system's time function. The generated entropy in pool 1 is then shifted to the pool 2.

The algorithm for entropy shifting is:

Start: Entropy Shifting

$k < 3$

Seeding

$h_A = \sum_{i=1}^{n} A_1$

Call seed function

$h_B = \sum_{i=1}^{n} B_1$

For $i = 1$

$C_1 = \sum_{i=1}^{n} A_1 + \sum_{i=1}^{n} B_1$

Else

$C_2 = \sum_{i=1}^{n} A_2 + \sum_{i=1}^{n} B_2$

Module 2 - Entropy Stretching

Pool 2 has its own generated entropy too. Pool 2 through a "Call Function" calls the entropy generated in pool 1 and the two generated entropies are concatenated (this is stretching). The stretching increases the number of bits to 128bits from 64bits each of the pools and hence increases the time to take to discover (if possible) the content of the entropy. Algorithm:

Start: Entropy Stretching

$j < 3$

For $j = 1$

$D_1 = (C_1 \bullet C_2)_1$

Else

$D_2 = (C_1 \bullet C_2)_2$

Module 3 - Entropy Mixing

The processes: entropy shifting and entropy stretching go through two rounds, and their resulting entropies which are entropy stretching(s) are XORed together to achieve "Entropy Mixing". Table 2 shows the result of a byte.

Input: $H' \& D$

Output: H

Start: Initialize Reseeding

$R = 0$

For $k < 3$

Call seed function

$H' = D_1 \oplus D_2 \ldots\ldots\ldots\ldots / \oplus = XOR$

$H = H' \oplus R \ldots\ldots\ldots\ldots\ldots / reseeding, R$

$R = H$

Table 2: Entropy Mixing – Mixing Bytes

Activity	Byte							
Entropy stretched result round 1	1	0	0	0	1	1	0	1
Entropy stretched result round 2	1	0	1	1	0	1	0	0
Final Entropy to be sent to TEA	0	0	1	1	1	0	0	1

The essence of entropy mixing is to make it difficult for the entropy (key) to be deciphered by cryptanalyst; hence making it difficult for encryption to be deciphered by hackers. The resulting entropy as the final entropy is then used as input to TEA for its encryption key generation as shown in Figure 5

4.0 RESULT

The developed entropy management technique for lightweight cryptographic smart home would assists in effectively guarding against related key attack, and hence, securing smart home from other forms of malicious attacks such as man in the middle, masquerading, eavesdropping, saturation, and Denial of Service (DoS) attacks

5.0 CONCLUSION

IoT provides ease of connectivity and computing capability for our everyday communication by ensuring effective data generation and exchange with minimal human intervention. Traditionally, security measures or sufficient cryptography functions for mitigating malicious attacks cannot be applied to low-capacity devices known as constrained devices connecting the IoT due to its low memory capacity and inability to accept antivirus software.

Therefore, the developed technique is expected to provide a secured smart home where smart home environments and appliances are protected as a result of effective key management, which invariably guard against related key attacks. The area of limitation of the research is its inability to provide security to traditional network setup and devices other than constrained devices.

REFERENCES

1. R. Dave, Tackling Data Security and Privacy Challenges for the Internet of Things, IoT W3C TechExpo, Berlin, 2016.
2. R. Karen, E. Scott, & C. Lyman, The internet of things: An Overview. Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC), 2015.
3. Jyotsna, P. G., Shradha, T., and C. Monika, Smart homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions. *International Research Journal of Engineering and Technology (IRJET)- Volume: 04* Issue: 05 | May - 2017, e-ISSN: 2395 -0056, p-ISSN: 2395-0072.
4. S. Daniel S. SEC Consult Vulnerability Lab – Vienna, Confidentiality Class: Public, Version: V1.0, 2016
5. U. Muhammad, A. M. Irfan, A. Imran, K. Shujaat & A. S. Usman. SIT: A Lightweight Encryption Algorithm for SecureInternet of Things. *International Journal of Advanced Computer Science andApplications, Vol. 8*, No. 1, 2017
6. A. Vassilev & T. A. Hall, "The importance of Entropy to information security," in Computer, vol. 47, no. 2, pp. 78-81, doi:120.1109/MC.2014. 47. 2014.
7. Whitewood Encryption System. Understanding and Managing Entropy. 2015.
8. M. B. Jordi, V. Athanasios, & G. Mariusz, Secure Smart homes: Opportunities and Challenges. ACM Comput. Surv. 50, 5, Article 75, 32 pages.https:// doi.org/10.1145/3122816. September 2017
9. B. B. Mario & W. Candid, Insecurity in the Internet of Things. 2015.
10. L. Gabriele, C. Salvatore & L. Erica, A Review of Systems and Technologies for Smart homes and Smart Grids, 2016, 9, 348.
11. B. Joseph, J. Andreas & Paul, On Privacy and Security Challenges in Smart Connected Homes, *European Intelligence and Security Informatics Conference*, 2016.
12. M. Somayya & D. Hema, Security Mechanisms for Connectivity of Smart Devices in the Internet of Things. 2016.
13. L. Greg. W. Beau & C. Joshua, Smart homes and the Internet of Things. *Atlantic Council, Brent Scowcroft Centeron International Security*. 2016.
14. Trend Micro, Implementing and Maintaining a Secure Smart home. Trend Micro, Incorporated. 2017.
15. B. Isha & L. Ashish, Analysis of Lightweight Cryptographic Solutions for Internet of Things. *Indian Journal of Science and Technology, Vol 9(28)*, DOI: 10.17485/ijst/2016/v9i28/98382..
16. K. Zetter, "Medical Devices that are Vulnerable to Life-Threatening Hacks", Wired, Retrieved from https://www.wired.com/2015/ 11/medical-devices-that-are-vulnerable-to-life-threatening- hacks/ on 11/02/2018..
17. BBC News, *German Parents Told to Destroy Cayla Dolls over Hacking Fears*, 2017. Retrieved from http://www.bbc.com/news/ world-europe-39002142 on 11/02/2018.
18. M. Nabeel, J. Zage, S. Kerr & E. Bertino, Cryptographic Key Management for Smart Power Grids Approaches and Issues. CS Department, CERIAS and Cyber Center, Purdue University. 2012.
19. M. Nicky, The Design Space of Lightweight Cryptography. 2015, Retrieved from https://hal. inria.fr/hal-01241013. On 07/03/2018.
20. Gary C. K. An Overview of Cryptography. 2018. Retrieved from https://www.garykessler. net/library/crypto.html. On 14/05/2018.
21. S. Zhou & Z. Xie, On Cryptographic Approaches to Internet-Of-Things Security (ZTE Corporation). Retrieved from https://www. semanticscholar.org/paper/8bc7e8a5288d900d3 753cf1094c952532e8d268e?p2df on 01/03/ 2018
22. T. Okamura, Lightweight Cryptography Applicable to Various IoT Devices. *NECTechnical Journal／Vol.12* No.1／Special Issue on IoT That Supports Businesses. 2017.
23. B. Tapalina, LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment. CSI Communications.www.csi-india.org. 2013
24. M. K .Youssouf, H. O. Siti, MD. S. Maheyzah & N. Herve, Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm. *IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 06*, Issue 06 (June. 2016), ||V1|| PP 01-07.
25. E. Mansoor, K. Shujaat & B. K. Umer, Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer*

Applications (0975 – 8887) Volume 61– No.20, January 2013.

26. K.V.G. Kiran, J. M. Sudesh, K. Sanath, &J. P. Viven, Design And Implementation Of Tiny Encryption Algorithm. *Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622,Vol. 5*, Issue 6, (Part -2) June 2015, pp. 94-97
27. S. Mohammad & K. G. Vishal, A crypt analysis of the tiny encryption Algorithm in key generation. *International Journal of Communication and Computer Technologies. Volume 01 – No.38,* Issue: 05 May 2013. ISSN NUMBER : 2278-9723
28. M. B. Abdelhalim, M. El-Mahallawy & A. Elhennawy. Design and Implementation of an Encryption Algorithm for use RFID System. *International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 2,* Issue 1, June 2013.
29. Vassilev & R. Staples. Entropy-as-a-Service: Unlocking the Full Potential of Cryptography. 2016. Doi:10:1109/MC.2016.275.
30. L. Patrick, R. Andrea R, Vincent S, Marion V. Analysis of the Linux Random Number Generator, Helsink University of Technology, Laboratory for Theoretical Computer Science, 2009.
31. R. Andrea, Pseudorandom Number Generators for Cryptographic Applications. Retreived fom https://www.rocq.inria.fr/secret/Andrea.Roeck/pdfs/dipl.pdf. On 05/03/2018.
32. Whitewood Encryption System. Understanding and Managing Entropy. 2015. Rereived from: https://www.blackhat.com/docs/us-15/materials/us-15-Potter-Understanding-And-Managing-Entropy-Usage-wp.pdf on 02/05/2018.
33. Vassilev & S. Staples, Entropy-as-a-Service: Unlocking the Full Potential of Cryptography. 2016. Doi:10:1109/MC.2016.275. Retreived from https://csrc.nist.gov/CSRC/media/Presentations/Entropy-as-a-Service-Unlocking-the-full-Potential/images-media/day2_demonstration_1100-1150pt2.pdf on 03/03/2018.
34. S. Mats, Design and Analysis of a Password Management System.Norwegian University of Science and Technology, Department of Electronics and Telecommunications, June 2014.

BIOGRAPHIES OF THE AUTHORS

Olushina Raphael OLUWADE

Olushina Raphael OLUWADE obtained his B.Sc. in Computer Engineering from Obafemi Awolowo University, Ile-Ife Osun State, Nigeria. He is currently a Masters Student of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria.

Olayemi Mikail OLANIYI (PhD)

Olayemi Mikail Olaniyi is a Senior Lecturer in the Department of Computer Engineering at Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BTech and M.Sc. in Computer Engineering and Electronic and Computer Engineering respectively. He had his Ph.D. in Computer Security from Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He has published in reputable journals and learned conferences. His areas of research include Computer security, Intelligent/ Embedded systems design and Applied Medical Informatics.

Yunusa Simpa ABDULSALAM

Yunusa Simpa Abdulsalam obtained his B.Eng. in Electrical/Computer Engineering and Masters of Computer Engineering in 2015 and 2017 respectively, from Federal University of Technology, Minna, Nigeria. He's currently a Ph.D. candidate in Data Science, Networking and Algorithm Thinking (DNA) at University Mohammed VI Polytechnic. He is a promising Computer Network Security expert. His research interests are in distributed systems design, wireless sensor networks, privacy and computer network security.

Lukman Adewale AJAO

Lukman Adewale AJAO is a Senior Research Fellow, currently working in the Department of Computer Engineering, Federal University of Technology, Minna, Nigeria. He obtained Postgraduate Diploma in Computer Science (2013) from University of Ilorin, Nigeria. Master of Engineering Degree (M.Eng) in Computer Engineering (2017) from Federal University of Technology, Minna, Nigeria. He is currently a Ph.D research associate in Computer Engineering at Ahmadu Bello University, Zaria, Nigeria. He is a corporate member of Nigerian Association of Technologist in Engineering (NATE), Member of IAENG, IACSIT & ISOC. His research interests are Real-Time Embedded System, IoT, WSN, FPGA and Machine Learning.