IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Issue-2, Feb 2020 E-ISSN: 2347-2693

Data Link Layer Encryption for The Internet of Things Using Elliptic Curve Cryptography Over Visible Light Communication Channel

D. Ene[1*], V.I.E. Anireh[2], D. Matthias[3]

[1,2,3]Dept. of Computer Science, Rivers State University, Port Harcourt, Nigeria

**Corresponding Author: donald.ene@ust.edu.ng*

DOI: https://doi.org/10.26438/ijcse/v8i2.5258 | Available online at: www.ijcseonline.org

Accepted: 10/Feb/2020, Published: 28/Feb/2020

***Abstract* -** The Internet as a fast-growing communication infrastructure comes with additional challenges of cybersecurity. A few techniques have been created to provide security in the application, transport, or network layer of a network. Many organizations have worked to provide security at higher OSI layers, from application layer right down to the network layers, without any at the Data Link layer. This has opened up many systems to a variety of compromises and attacks. This study proposes the provision of the public key Elliptic Curve Cryptography to serve the Data Link Layer instead of the Media Access Control (MAC). In this study, visible light communication technology for fast data communication and secure data transmission on the data link layer using public-key cryptosystem are discussed. The visible light communication technology consists of Light Emitting Diodes (LED) that flicker at an incredibly high frequency, thereby enabling a very high-speed wireless communication and an elliptic curve encryption component that carries out an integrated encryption scheme using Elliptic Curve Integrated Encryption Scheme (ECIES) and a digital signature algorithm using Elliptic Curve Digital Signature Algorithm (ECDSA). For the data link layer security, the encryption procedure is applied to the communications server and the programmable circuit boards (PCB) controlling the visible light communication devices. While the complete system model was implemented in a program, a prototype of the architecture was implemented on a microFourQ-MSP-IAR Embedded Workbench IDE-MSP430 7.12.4, and Wolfram Mathematica. Two advantages of visible light communication and public-key encryption were demonstrated: 1) providing security for the data link layer messages. 2) using VLC to speed up the encryption and decryption process in the data link layer.

***Keywords*:** Internet of Things, Simulated Systems, Visible Light Communications, Elliptic Curve Cryptography, VLC, ECC, IoT, OSI, Data Link Layer, PKI

I. INTRODUCTION

The International Standards Organization (ISO) proposed and developed the Open Systems Interconnection reference model in 1984 to serve as the most basic element of computer networking. This is a layered framework conceptualizing how communications should be done between heterogeneous systems. The OSI concept defines an architecture that logically divides the roles required to support system-to-system communication.

The seven layers of the OSI model each has a separate level of abstraction, and these layers each perform a well-defined function to carry out the communication [1].

The layered approach was adopted so that networking functions can be separated into smaller logical pieces. This way data communication problem can be easily isolated and solved using the divide-and-conquer method [2].

The data link layer is the second layer among the seven layers of the Open System Interconnection, saddled with the responsibility of transferring data frames reliably from node to node. This layer primarily deals with raw data transmission to the network layer. Data communication is done by splitting data into small fragments known as packets, and then the data link layer serves the frames to the network layer [3].

The frames are simply the physical hardware address of each network interface card connected to the network. Token Ring, ARCnet, and Ethernet are types of local network data link protocols. The network uses other data link protocols such as Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) if data communication extends beyond the local network onto the Internet [4].

Blocks of data with the necessary bit error detection and correction, synchronization, flow control, and error control are sent by the data link layer. This layer is also responsible for creating and recognizing frame boundaries since the physical layer only accepts and transmits a stream of data without any regard to the meaning and the structure.

The rapid growth of wireless communications has raised a serious concern for network security. Some approaches have been established to ensure security in the application, transport and network layers of the Open System International (OSI) model. Numerous organizations have joined safety efforts at higher OSI layers, from application layer right down to the network layer. In any case, one region largely left unattended is the hardening of the Data Link layer [5].

Data transmission over the network is carried out with the data being fragmented into small packets. The data link layer provides service to the network layer which is the next layer above it. The communication channel that interfaces the connecting nodes is referred to as links, and for the datagram to move from source to the destination, the datagram must be moved across an individual link. The Data link layer protocols describe the format of the packet exchanged across the nodes as well as the services such as Error detection, retransmission, flow control, and random access [6].

The data link layer is further divided into two sub-layers namely the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The role of the LLC sublayer, as described by the Institute of Electrical Electronics Engineers working group 802 (IEEE-802) Local Area Network (LAN) specification, is to control the flow of data between various services and applications, and then provide error notification and acknowledgement mechanisms. The logical link control sublayer then talks to the MAC sublayers, whose duty is to the physical media for transport. The LLC sublayer is also responsible for physically addressing the frames. The common types of the MAC sublayer include wired and wireless specifications.[7]
The radio-based wireless network, Wireless Fidelity (Wi-Fi) is one among the foremost engaging networks that are growing rapidly with straightforward and quick implementation and setup. A lot of users are considering deploying this sort of network than the wired version. The next section presents safety loopholes in the wireless network as it affects the data link layer by reviewing its security protocols and mechanism. Security protocols like the Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and 802.11i, and mechanisms like the MAC access management list; their vulnerabilities and existing tools to take advantage of these vulnerabilities. Knowing how this mechanism and protocols work, as well as its weakness and vulnerabilities, are often very useful for designing, and implementing the secure optical wireless network so as to effectively minimize the impact of the attack on the data link layer of IoT devices. Securing the data link layer has become imperative due to the constant evolution and continued independence of the smart devices [8].

The following sections of this paper are structured as follows: Section I contains the introduction, introducing the subject and its relevance. Section II presents relevant works related to wireless network encryption. Section III presents the methods, materials and approach followed to achieve the study. Section IV explains how the proposed study was implemented, and its output result.

II. RELATED WORKS

There are different methods an attacker may attempt to use on the data link layer. The aim of the attacks is basically to compromise availability, confidentiality or availability of information. More often than not, the attacks on the data link layer always succeed due to the vulnerability inherent in that layer. One of such vulnerabilities is the lack of fine-grain control for the data link layer [9].

The data link layer may not be considered a novel platform for attacks; however, this layer continues to trouble internet-connected systems. The tools enumerated by [10] used to implement the data link layer attacks rely on a specific attack vector, which is the lack of proper authentication during data communication. However, the attack vectors for the wireless network are somewhat different from that of the wired network. The attack vectors in the wireless network include; the hidden node attack, deauth, and fake access point attack [11].

While investigating the attacks that are unique to the wireless network, [12] identified the signatures and the tools used for implementing the attacks.

Although not enough, security in wireless networks has been significantly enhanced by the Institute of Electrical Electronic Engineers (IEEE) 802.11i (Radius) standards. Confidentiality, integrity, and authenticity attack vectors still exist in Ethernet wired and wireless networks as it relates to the data link layer [13].

Li-Fi, which is a form of Optical Wireless Network that uses Light Emitting Diode (LED) [14]. The cryptographic algorithm used in Li-Fi is Caesar Cypher wheel Algorithm.
The capability available in IoT devices is what informs the choice of cryptographic algorithm used to secure the devices [15,16]. However, none of the aforementioned network security apparatus solved the weakness inherent in the data link layer on the wireless network. However, light, which is the basis of the visible light communication is not susceptible to electromagnetic interference. Therefore, the error rate during data transmission in the data link layer is negligible.

III. METHODOLOGY

The methodology adopted for this study was constructive research, unlike other types of study, does not require empirical validation [17]. Using this procedure, a system is developed and then assessed. This is done by constructing artefacts and knowledge using practical potential values. The constructive study contributes to a new technique, algorithm, framework, or theory that solves a domain-specific problem, and the result will further build more knowledge [18].

Data Link Layer Security for the Internet of Things using Elliptic Curve Cryptography over Visible Light Communication targets knowledge to mitigate the insecurity in IoT on the data link layer.

In the design of the system, a parallel structure was carried out in the algorithm to meet the real-time requirements. Preferably, parallelism at the design level needs to be applied minimally to have a carefully designed, nonspecific structure that can work on any programmable circuit board (PCB). When a PCB of that kind is used, an optimization can be carried out for that device. Those kinds of optimizations are often transparent to the user due to the sophisticated synthesis tool currently available with different vendors of the visible light communication systems.

The design directions are as follows:

i. The most suitable algorithm should be selected for designing signature IP blocks with reference to the large-scale application requirements, which are: high-security level, low consumption, and maximum throughput.
ii. The algorithm for key generation, signature generation, and signature verification should be defined and specified.
iii. The different IP and the choice of a standard interface should be specified
iv. System-level security and throughput performance evaluation
v. Hardware and software co-simulation of the entire signature processor and performance evaluation

Following the above order, we review the architecture in Figure 1. The transmitter section consists of an LED which acts as a communication source. VLC is implemented using White LED bulbs at the transmitter. This kind of devices is generally used for illumination by applying constant current on it. When the LED is ON, then it transmits digital string 1 and when it is OFF then it transmits the string 0. And the rate of encoded data depends on the flicker of LED. The input can be any type of data. When a constant current is applied to a LED, a certain amount of energy (photons) gets released, that we perceive as visible light. If the input current to the LED is varied slightly, the intensity of the light output also varies.

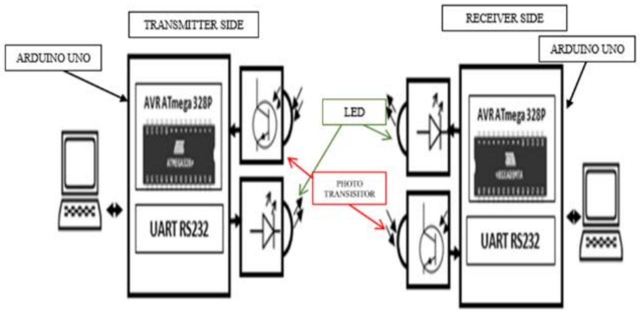

Figure. 1. VLC Architecture
Source: Arya College of Engineering & I.T, Jaipur (Raj.), India

Since ECC security depends on the ability to calculate point multiplication [19], the Montgomery algorithm will be adopted so that point doubling and point addition parallelism can be achieved and then computed independently. These operations are based on modular arithmetic operations. Although the point multiplication needs six multiplications, and point addition needs five multiplications, only two multiplications will be used in each operation.

In figures 2a and 2b, the components enclosed in dotted lines are indicated: one involves calculations and the other involves data processing. The fundamental activity in the first one involves scalar multiplication. The subsequent one carefully executes the KDF module (which produces the keys K_{MAC} *and* K_S), E and MAC. Depending on the operation performed, whether encryption or decryption, the MAC data source is different.

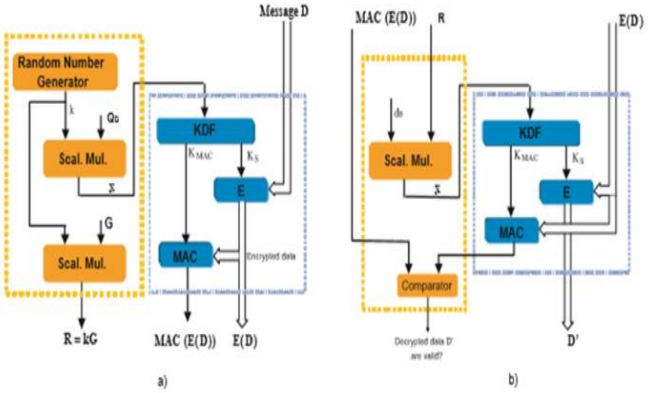

Figure 2. ECIES architecture for encryption and decryption
Source: National Institute for Astrophysics, Optics and Electronics, Puebla

The data flow for signature verification in the ECDSA, and signature generation are indicated in Figure 2. For signature verification, just the scalar multiplication *kG* is calculated; *k* is an arbitrary figure and *G* the mutual element in tuple *T*. A modular reduction to the *x*-coordinate of kG is applied to the first segment of the signature, r. The signature, *s*, which is the second part, is acquired from modulo *n* calculations, which involves the hash of input data e, the r-value, the private key d_A, and the arbitrary number k. Two scalar multiplications are computed in a signature verification.

These scalars are the derivatives of modulo n procedures concerning the hash value of incoming data, and the incoming signature under test. The points are the public key Q_A of the communication source and the shared point G. A sum of points is also required besides the signature generation; to determine if the signature is valid, the x-coordinate of this point sum is used.

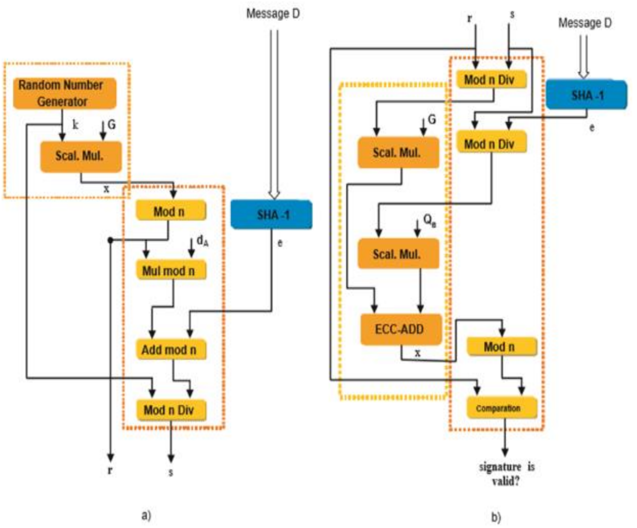

Figure. 3. ECC architecture for signature generation and verification
Source: National Institute for Astrophysics, Optics and Electronics, Puebla

The following section examines the proposed system's architecture. An architecture to support both ECIES and ECDSA schemes is designed for the encryption and decryption process in the data link layer over the VLC. The system is made up of two main structures: one for arithmetic operations and other processing data while the process is in progress without interrupting the run.

The proposed system architecture includes employment of the elliptic curve cryptographic schemes ECDSA and ECIES and the VLC module.

This architecture improves security in the area of the dotted lines, which is the area where the physical and data link layers are located. The module within the dotted lines are responsible for the data communication and signal processing and transfer, which is the area that is the main focus of this study.

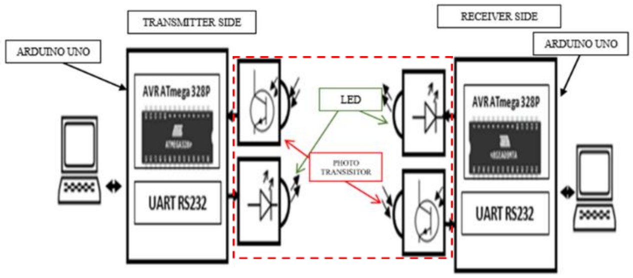

Figure 4. The architecture of the Proposed System

Elliptic Curve Digital Signature Algorithm (ECDSA) is applied to ECC to make it appropriate for security encryption. The Secure Hash Algorithm 1 (SHA-1) is an algorithm for harsh operation in the signature generation and verification of the ECDSA [10]. SHA-1 is a one-way, but iterative hash function that generates a 160-bits representation called message digest [10]. SHA-1 can be defined in two phases: preprocessing and hash function or hash operation. Preprocessing is carried out by message padding, and then the padded message is parsed into 512-bit blocks, and then initialization values are set to be used in the hashed operation. Parsing is done to ensure the padded message is in a multiple of 512-bit blocks. For instance, padding means adding the 1 bit to the length of message D in the bits as a 64-bit number. zeros are added to fill a 512-bit block, then the padded message is parsed into $N\ B$ 512-bit blocks, $D^{(1)}, D^{(2)}, \ldots, D^{(N\ B)}$. The initial value, $H^{(0)}$, comprised of the following five 32-bit words in hexadecimal:

$H_0^{(0)} = 0x67452301$
$H_1^{(0)} = 0xefcdab89$
$H_2^{(0)} = 0x98badcfe$
$H_3^{(0)} = 0x10325476$
$H_4^{(0)} = 0xc3d2e1f0$

Starting with $H^{(0)}$, every value $H^{(i)}$ of block $D^{(i)}$, $1 \leq i \leq NB$ is used to calculate the next hash value $H^{(i+1)}$ consistent with the next block $D^{(i+1)}$.

A message schedule is generated by the hash computation for the padded message and uses the schedule, along with the constants, functions, and word operations to iteratively generate a series of other hash values, one for each 512-bit block. the result of the final block then becomes the message digest after these 512-bit blocks are processed in 80 iterations each.

Algorithm 1 HASH operation: SHA-1 Core
Input: $D^{(i)}$ a block of 512-bit
Output: The corresponding HASH value to $D^{(i)}$ from $H^{(i-1)}$

```
1: The message schedule is prepared, $W_t$ from block $D^{(i)}$
```

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) & 16 \le t \le 79 \end{cases}$$

```
The five working variables A, B, C, D, and E are initialized, with the (i-1)st hash value:
    $A \leftarrow H_0^{(i-1)}$
    $B \leftarrow H_1^{(i-1)}$
    $C \leftarrow H_2^{(i-1)}$
    $D \leftarrow H_3^{(i-1)}$
    $E \leftarrow H_4^{(i-1)}$
for $t$ form 0 to 79 do do
    $E \leftarrow D$
    $D \leftarrow C$
    $C \leftarrow ROTL^{30}(B)$
    $B \leftarrow A$
    $A \leftarrow ROTL^{30}(A) + f_t(B,C,D) + E + k_t + W_t$
end for
Compute the $i$th intermediate hash value $H^{(i)}$:
    $H_0^{(i)} \leftarrow A + H_0^{(i-1)}$
    $H_1^{(i)} \leftarrow B + H_1^{(i-1)}$
    $H_2^{(i)} \leftarrow C + H_2^{(i-1)}$
    $H_3^{(i)} \leftarrow D + H_3^{(i-1)}$
    $H_4^{(i)} \leftarrow E + H_4^{(i-1)}$
```

In algorithm 1 above, hash computation is applied to every block of $D^{(i)}$. After the block $D^{(NB)}$ is processed, the resulting 160-bit message digest of the data set in D becomes $H_0^{(NB)} \parallel H_1^{(NB)} \parallel H_2^{(NB)} \parallel H_3^{(NB)} \parallel H_4^{(NB)}$, where $\parallel$ stands for a bit-string concatenation. Operation $ROTL^i(A)$ in the algorithm means a left shift of value *Aj* positions.

The function $f_t(B,C,D)$ is defines as

$$f_t(B,C,D) = \begin{cases} (B \wedge C) \oplus (\neg B \wedge D) & 0 \le t \le 19 \\ (B \oplus C \oplus D) & 20 \le t \le 39 \\ (B \wedge C) \oplus (B \wedge D) \oplus (C \wedge D) & 40 \le t \le 59 \\ (B \oplus C \oplus D & 60 \le t \le 79 \end{cases}$$

Also, the for 32-bit constants k_t are defined as

$$k_t = \begin{cases} 0x5a827999 & 0 \le t \le 19 \\ 0x6ed9eba1 & 20 \le t \le 39 \\ 0x8f1bbcdc & 40 \le t \le 59 \\ 0xca62c1d6 & 60 \le t \le 79 \end{cases}$$

using affine coordinates for an elliptic curve defined on F_{2^m}, the function ECC-DOUBLE is carried out according to algorithms 2 and ECC-ADD are carried out according to algorithm 3. ECC-ADD involves two multiplications, one inversion, eight additions, and one square. The operations ECC-DOUBLE involves two multiplications, one inversion, five additions, and two squaring all of which operate on F_{2^m}.

Algorithm 2 ECC-ADD: Sum of different points

```
Input: $P = (x_1, y_1), Q = (x_2, y_2), x_1, y_1, x_2, y_2 \in F_{2^m}$
Input: $a \in F_{2^m}$, a is the constant in the elliptic curve
Output: $R = x_3, y_3 = P + Q$
if $P = O$ or $Q = O$ then
    $R \leftarrow O$
    Return
end if
$\lambda \leftarrow (y_2 + y_1)/(x_2 + x_1)$
$x_3 \leftarrow \lambda^2 + \lambda + x_1 + x_2 + a$
$y_3 \leftarrow \lambda(x_1 + x_3) + x_3 + y_1$
return
```

Algorithm 3 ECC-DOUBLE: Double of a Point *P* (Point Doubling)

```
Input: $P = (x_1, y_1), , x_1, y_1 \in F_{2^m}$
Input: $a \in F_{2^m}$, a is the constant in the elliptic curve
Output: $R = (x3, y3) = 2P$
if $P = O$ or $Q = O$ then
    $R \leftarrow O$
    return
end if
$\lambda \leftarrow x_1 + y_1/x_1$
$x_3 \leftarrow \lambda^2 + \lambda + a$
$y_3 \leftarrow x_1^2 + \lambda x_3 + x_3$
return
```

Datalink layer algorithms may be embedded in the network hardware rather than running as a software process in a machine. Usually, computer algorithms do not have to run as software on general-purpose machines. Dedicated hardware can be designed to run them. However, in this section, the focus is the algorithm, whether embedded or as a software process.

The key function of the data link layer is to receive data packets from the network layer (layer 3) and convert them to the frames that are ready to be transmitted by the physical layer. In the frame, there are sender's and receiver's network addresses, as well as error checking, and control information. The mode of communication employed in this study minimizes errors during transport, unlike radio-based wireless network.

IV. RESULTS AND DISCUSSION

Different bit range of the ECC curve is presented in Table 1 with the execution time of different elliptic curve cryptographic functions, such as key generation, encryption time, and decryption time for 31 bytes of data over radio-based wireless network and VLC. Analyzing the cost of key generation against the curve, it was discovered that both are directly relative. The cost of key generation time increases in relation to the increase in bit length of the curve, with a clear difference in both Wi-Fi and VLC.

The results of the execution time for the cryptographic scheme ECDSA on the data link layer over VLC are also presented. The results obtained were simulating the overall system. The architecture was tested with Wireshark logs as data link layer data sets. Signatures were generated and verified; also, files were encrypted and decrypted. The results were compared with the results of the radio-based wireless system.

Table 1. Execution Time Result from System

Curve	**Key Generation Time** **(s)**		**Encryption Time** **(s)**		**Decryption Time** **(s)**	
	Wi-Fi	VLC	Wi-Fi	VLC	Wi-Fi	VLC
NIST 163	0.04336	0.004	0.089972	0.0083	0.087804	0.0081
NIST 233	0.114904	0.0106	0.201624	0.0186	0.174524	0.0161
NIST 283	0.114904	0.0106	0.321948	0.0297	0.321948	0.0297
NIST 409	0.246068	0.0227	0.68292	0.063	0.592948	0.0547
NIST 571	0.519236	0.0479	1.606488	0.1482	1.660688	0.1532

The above table data is further represented in a graph in Figure 5. The bar chart shows the result of execution time in the system, plotting tasks against time.

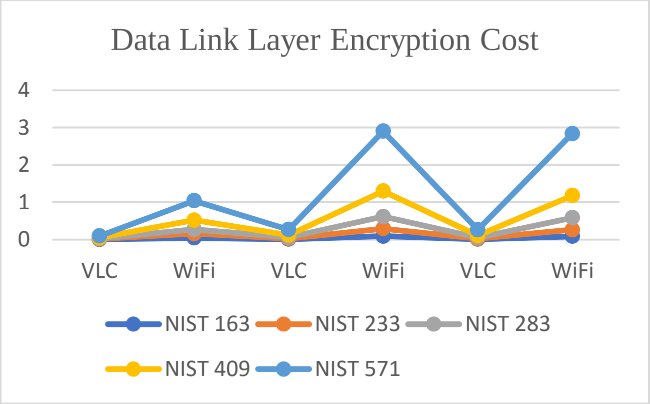

Figure 5. Graph execution Time Result

Table 1 shows the timing of key generation, encryption and decryption time of data in the data link layer over the visible light communication, and Wi-Fi network. In a key generation, encryption, and decryption time for VLC shows a significant improvement over the Wi-Fi. This shows that in term of bandwidth, the proposed system outperforms the existing system when it comes to data link layer encryption and overhead on the network.

Analysis of the cost of encryption against different lengths of curves concludes that they are directly proportional. The length of the bit also increases as the increase in the encryption cost; however, this increase is more so rapidly than the cost of key generation. Analysis of the cost of decryption against curves also gives an idea that they are directly proportional. Decryption cost also increases as the increase in bit length of the curve; however, this increase is too much exponential as compared with other two costs. It can be concluded that the key generation is the least costly process in ECC over VLC. Although encryption and decryption take more time, they still take less time to complete the chain of processes compared to another public-key cryptosystem such as RSA, and therefore good for the purpose of securing data link layer communication of the IoT devices. The result so far discussed are also presented graphically in Figure 5 for easy visual representation.

This study focused majorly on data link layer security for IoT over VLC as a medium and ECC as a preferred security apparatus for securing the IoT communication on the visible light spectrum. The reason ECC was preferred is due to its smaller key size, and fast decryption process. This is because IoT devices come with smaller storage capacity [20], and low processing power, such as smart cards, and embedded systems (Television set, Refrigerator, Smartphones, Home Security System, etc.) that is why ECC is recommended for the purpose. Considering that there are affordable devices that can break RSA keys smaller than 1024 bits within 72 hours, the cost of key generation can be considered as a factor in the choice of public-key systems to use when using digital signatures, especially for smaller devices with less computational resources than our simulator. This means less heat, less power consumption, less real estate consumed since it runs on the printed circuit board, and software applications that run more rapidly and make lower memory demands. Leading in turn to more portable devices which run longer, and produce less heat.

When it comes to network bandwidth, the main concern relates to the symmetric algorithm used for Message Authentication Coding (MAC) for message integrity checking in the data link layer. This, however, has nothing to do with the choice of cryptosystem used. Characteristically, embedded systems that are smaller more frequently start sessions, here, the asymmetric authentication may constitute a larger percentage of the overall traffic and the signature and key sizes can negatively impact the network. This is the reason the Visible Light Communication (VLC) is preferred over the existing wireless network where bandwidth and errors are issues. The key size generally may have no impact on performance, but size matters when it comes to the cost of secure storage of the keys on the processor of the printed circuit board (PCB) of the optical wireless network.

In our proposed work, we have introduced a public key cryptosystem to secure the data link layer for preventing and mitigating attacks during connectivity. This solution seeks to provide integrity and authenticity for the data link layer messages with VLC as a medium of communication.

V. CONCLUSION AND FUTURE SCOPE

Data link layer security has become a concern with the rapid evolution, growth, and continuous independence of the IoT. Rigorous research has been made to secure the data link layer using public-key cryptosystem based on elliptic curve driven by a visible light communication system for secure data communication in IoT devices. Bandwidth is already becoming an issue for the connected system, if the proposed public-key cryptosystem is deployed over the existing wireless network, it will negatively impact the network thereby making smooth communication impossible. In this study, we simulated the ECC encryption process over the visible light communication, and in our experimental result, we have shown different encryption and decryption time over Wi-Fi and VLC, and we conclude that ECC over VLC is preferred as they save substantial time. The future work will be focused on running the encryption in a server and getting signatures verified in the programmable circuit boards housing the transceivers of the LED access points.

REFERENCES

[1] G. Bora, S. Bora, S. Singh, & S.M. Arsalan, OSI reference model: An overview. *International Journal of Computer Trends and Technology (IJCTT)*, **Vol 7 Issue 4**, pp.214-218, **2014.**

[2] Y. Li, D. Li, W. Cui, and R. Zhang, *"Research based on OSI model."* In the proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (3ICCSN - 2011), Xi'an, **China**, pp.**554-557**, **2011.**

[3] N. Briscoe, "Understanding the OSI 7-layer model." *PC Network Advisor* **Vol 120 Issue 2**, pp.13-16, **2000.**

[4] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J.V. Randwyk, and D. Sicker, Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. In *USENIX Security Symposium* **Vol. 3**, pp. 16-89, **2006.**

[5] S. M. AlMheiri and H. S. AlQamzi, "Data link layer security protocols in Wireless Sensor Networks: A survey," 2013 10th Ieee International Conference on Networking, Sensing and Control (ICNSC - 2013), pp.**312-317, 2013.**

[6] M. Meribout and A. Al Naamany, "A collision-free data link layer protocol for wireless sensor networks and its application in intelligent transportation systems," *2009 Wireless Telecommunications Symposium*, Prague, pp.**1-6**, **2009.**

[7] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello and M. Rossi, "Low power link layer security for IoT: Implementation and performance analysis," *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sardinia, pp.**919-925 2013.**

[8] A. Annapurna, S. Madhuri, & D. Mohammed. Data Link Layer Security Issues. *International Journal of Computer Science & Engineering Technology*, **Vol 4 Issue 7**, pp.1009-1102, **2013.**

[9] B. Alotaibi, & K. Elleithy. A New MAC Address Spoofing Detection Technique Based on Random Forests, *Sensors*, **Vol 16, Issue 681,** pp.1-14, **2016.**

[10]T. OConnor, Detecting and Responding to Data Link Layer Attacks. Boston: SANS Institute 2019.

[11]K. Singh, Security Issues in Wireless Networks. Research Gate, **pp. 1-5, 2014.**

[12]K. Tao, J. Li, & S. Sampalli, Detection of Spoofed MAC Addresses in 802.11 Wireless Networks. Springer, **Vol 1, Issue 23,** pp.201-213, **2008.**

[13]L. Wong, An Overview of 802.11 Wireless Network Security Standards; Mechanisms. Swansea: SANS Institute, **2005.**

[14]H. Haas, Li-Fi - "Shedding Light on Future Wireless Communications." *2011 TED Conference*, Edinburgh. **2015.**

[15]J. Patel, F. Suthar, & S..V.O. Khanna, "A Critical Analysis on Encryption Techniques used for Data Security in Cloud Computing and IoT (Internet of Things) based Smart cloud storage System: A Survey," International Journal of Scientific Research in Network Security and Communication, **Vol.7**, **Issue.2**, pp.21-25, **2019.**

[16]E.I. Davies & V.I.E. Anireh, Design and Implementation of Smart Home System Using Internet of Things. Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech, **Vol 7, Issue 1,** pp.22-42, **2019.**

[17]A. Oyegoke, The constructive research approach in project management research. International Journal of Managing Projects in Business, **Vol 8, Issue 5/6,** pp. 573–595, **2011.**

[18]G. Crnkovic, Constructive Research and Info-computational Knowledge Generation. Springer, **Vol 314, Issue 1,** pp. 359–380, **2010.**

[19]M. Morales-Sandoval, Hardware architecture for elliptic curve cryptography and lossless data compression. Puebla: *Computer Science Department National Institute for Astrophysics, Optics and Electronics*. **pp. 1-89, 2004.**

[20]R.Piplode, P. Sharma and U.K. Singh, "Study of Threats, Risk and Challenges in Cloud Computing," *International Journal of Scientific Research in Computer Science and Engineering*, **Vol.1**, **Issue.1**, pp.26-30, **2013.**

Author's Profile

D. Ene pursued B.Sc. in Network Computing from Oxford Brookes University, UK, and M.Sc. in Computer Science in the Rivers State University. He is a member of IEEE and a member of Computer Professionals of Nigeria. He has designed and implemented different projects in the public and private sectors across Nigeria especially in the telecommunication industry. He is currently a Technologist in Rivers State University, Port Harcourt, Nigeria. His main research work focuses on Wireless Networks, Artificial Intelligence, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, and IoT.

V.I.E. Anireh pursued B.Sc. in Computer Science at the University of Nigeria, and M.Sc., and PhD from the University of Port Harcourt. He is a research fellow, senior faculty member, and currently the Head of Department of Computer Science in the Rivers State University, Port Harcourt, Nigeria. He is a member of IEEE and a member of Computer Professionals of Nigeria. He has many scholarly publications in both local and international journals. His main research work focuses on Artificial Neural Networks, Machine Learning, Computer Networks, IoT, and Big Data.

D. Matthias pursued B.Sc. in Mathematics/Computer Science at the University of Port Harcourt, Rivers State, M.Tech. from the Federal University of Technology Owerri, Nigeria and PhD from the Rivers State University of Science and Technology, Port Harcourt, Nigeria. He is currently a senior lecturer in the Department of Computer Science in the Rivers State University. He is a member of Computer Professional of Nigeria (CPN) since 2010 and a life member of Nigeria Computer Society (NCS) since 2012. He has published more many research papers in reputed international journals and conferences. His main research work focuses on Computational Theory, Expert System, Big Data, Software Development, Deep Learning and Networking.