Covenant Journal of Informatics & Communication Technology. Vol. 11, No. 01,June, 2023
ISSN: ***print*** **2354 – 3566** ***electronics*** **2354 – 3507 DOI:**

An Open Access Journal Available Online

A Survey of Lightweight Cryptosystems for Smart Home Devices

[1]Olayemi Mikail Olaniyi, [2]Abraham Ayegba Alfa, [1]Idris A. Dauda, [1]Bello Abdulaziz

[1]Department of Computer Engineering, School of Electrical Engineering and Technology,
Federal University of Technology, Minna, Nigeria.
[2]Department of Computer Sciences, Faculty of Computing and Informatics,
Confluence University of Science and Technology, Osara, Nigeria.
mikail.olaniyi@futminna.edu.ng, alfaaa@custech.edu.ng ,
bello.m1605299@st.futminna.edu.ng

Received: December 11, 2022, Accepted: June 15, 2023

Publication: June, 2023

Abstract—A Smart Home uses interconnected network technology to monitor the environment, control the various physical appliances, and communicate with each other in a close environment. A typical smart home is made up of a security system, intercommunication system, lighting system, and ventilation system. Data security schemes for smart homes are ineffective due to inefficiency cryptosystems, high energy consumption, and low exchange security. Traditional cryptosystems are less-applicable because of their large block size, large key size, and complex rounds. This paper conducts a review of smart homes, and adopts Ultra-Sooner Lightweight Cryptography to secure home door. It provides extensive background of cryptography, forms of cryptography as associated issues and strengths, current trends, smart home door system design, and future works suggestions. Specifically, there are prospects of utilizing XORed lightweight cryptosystem for developing encryption and decryption algorithms in smart home devices. The Substitution Permutation Network, and Feistel Network cryptographic primitives were most advanced forms of cipher operations with security guarantees. Therefore, better security, memory and energy efficiency can be obtained with lightweight ciphers in smart home devices when compared to existing solutions. In the subsequent studies, a blockchain-based lightweight cryptography can be the next springboard in attaining the most advanced security for smart home systems and their appliances.

Keywords/Index Terms—Lightweight, Smart Home, Cryptography, Cryptosystem, Encryption, Decryption, Security, Performance

1. Introduction

Smart homes offer improved services to occupants of buildings that are often referred to as automated homes (Sovacool & Rio, 2020). Smart technologies comprise things, devices or equipment which are capable of being digitally connected, autonomous and automated to a large extent. In automated buildings, there are interfaces to support the monitoring, controlling and detection of devices such as lighting ventilation, heat and air conditioning, hardware and security systems (Fakroon et al., 2020). At present, smart systems are composed of switches and sensor to facilitate communication across centralized axis known as gateways.

In fact, majority of gateways are control systems which are design with user interface and the communication network managed with Internet of Things (IoT). It implies that the digital devices in automating homes system should be able to access the Internet in order to afford their users the opportunity to monitor, control, manage, and automate diverse household electronics (Zaidan & Zaidan, 2020). The drawbacks of smart home technologies (SHTs) are the security and privacy exploitations and power computation, which has potentially put citizens' privacy at risk. Consequently, there are cases of users' information leak and uncontrolled breach of privacy.

Artificial Intelligence (AI) methods were introduced to reduce breach risks and leakage (Ogundokun et al., 2022; Alfa et al., 2022). To minimize the leakage of information from these technologies, machine learning was introduced to regulate communication between smart devices and Internet (Ogundokun et al., 2022). Also, application of AI methods for data protection in SHT could help to determine compromised data encrypted in a traffic by using pattern-matching techniques (Balas, Kumar & Srivastava, 2020). The intelligent process for IoT-based smart home applications has numerous benefits. However, these technologies are not perfect solutions to communication network delivery (Zaidan & Zaidan, 2020).

Security and privacy have serious concerns in SHTs, for these reasons, cryptosystem was deployed. A cryptosystem uses a set of algorithms to transform plaintext to ciphertext. The traditional cryptosystems approach of providing protection through a complex algorithm are ineffective, because they consume more energy, and space leading to lesser efficiency in smart devices and home appliances. The main contributions of this survey paper include:

1. To explain the fundamentals of cryptosystems.
2. To present the trends of lightweight cryptography in secure smart homes devices
3. To present a formal design for secure smart home system architecture based on Ultra-Sooner lightweight cryptography
4. To identify and suggest future research works for securing smart home systems

The subsequent sections of this paper are arranged as follows (Misra, 2021): Section 2 presents fundamentals of cryptography, Section 3 Trends of lightweight cryptography in smart home devices. Section 4 Secure Smart home system architecture. and Section 5 concludes the paper.

2. Fundamentals of Cryptography

The traditional ciphers have huge key size, large block size and complex rounds (Fakroom et al., 2020; Balas Kumar & Srivastava, 2020). Often, cryptosystems are used to describe means and techniques of data conversation in a secure form, that is, the data cannot be used or modified by unauthorized adversary. Thus, authenticity of the data can be established, modification on the data can be avoided and the data cannot be repudiated by the generator. A Cryptosystem consists of five-tuples (P_T; C_T; P_K, E_C, D_C), must satisfy the following conditions (Padhye & Saraswat, 2018):

1. P_T is a finite set of possible Plaintexts.
2. C_T is a finite set of possible Ciphertexts.
3. P_K is a finite set of possible keys.

For each key k Є P_K, there is an encryption condition E_k Є E_C, E_k: $P_T \rightarrow C_T$ and a decryption condition D_k Є D_C, D_k: $C_T \rightarrow P_T$ such that, for any plaintext y Є P_T, $x = E_k(y)$ is the corresponding ciphertext and $D_k(E_k(y)) = y$.

It follows from the above conditions that, in a valid cryptosystem, the encryption must be invertible since the decryption function is the inverse of the encryption function. Cryptosystem cares about privacy/confidentiality, authentication, integrity and non-repudiation (Sharma, 2020). This cryptosystem technique requires large memory consumption and huge buffer size. Hence, it becomes more complicated in embedded devices such as RFID tags and sensors in wireless networks (Thangamani & Murugappan, 2019). However, lightweight cryptosystem schemes were developed to inspire embedded systems to comply with the processing capability and latency requirements of end devices while fulfilling the security requirements (Sarker, Gia, Tenhunen, & Westerlund, 2018). Cryptosystem have basic components these includes encryption, decryption, exclusive or gate and block cipher which are discuss as follows:

Encryption is a process of converting confidential data into indecipherable form by following confusion and diffusion strategies (Majumdar & Dutta, 2020; Rana et al., 2021). Encrypted data is known as ciphertext, while unencrypted data is commonly referred as plaintext (Shouran, Ashari & Priyambodo, 2019). Fortunately, encryption is a technique for securing the overall systems, the lightweight cryptosystem needs to adopt a method that is evaluated as ensuring sufficient security in cryptography environment (Pandurang, 2020). It is undoubtedly important to have successful decryption schemes while designing a strong encryption algorithm (Majumdar & Dutta, 2020). However, decryption was the reversed of encryption scheme, in which, its converts cipher text to plaintext (Mustafa et al., 2018). Cryptographic algorithms transform confidential data from readable form to protected form and back to readable form. There are different types of cryptographic algorithms with different operational behaviours.

2.1 Secret Key Cryptography

Secret Key Cryptography known as symmetric key cryptosystem in which a single key is used for encryption and decryption (Chaoyun, 2020). The source encrypts the data by using the protected key and the single key is used by the destination to decrypt the data. The source and destination exchange the key by a protected channel to start communication. Symmetric encryption uses three types of algorithms based on block, stream and hashing ciphers (Pandurang, 2020).

Block Cipher: Block ciphers are basic primitives in cryptosystem from which many other systems are built. Block ciphers encrypt an entire block of plaintext bits at a time. The Message Authentication Codes (MACs), stream ciphers, hash functions and authenticated encryption schemes are design from block cipher (Sehrawat & Gill, 2018; Yoshizawa & Preneel, 2019; Sehrawat & Gill, 2019). Traditional block cipher include: Advanced Encryption Standards (AES) and Data Encryption Standard (DES) (Pandurang, 2020).

Stream Cipher: It encrypts bit individually. Present stream ciphers enjoy efficient implementations and more importantly, high throughput and extremely high speed compared with block ciphers. The incredible performance makes dedicated stream ciphers be the favorite encryption algorithms in communication infrastructures, such as the 2G to 5G mobile communications and TLS (Sehrawat & Gill, 2018).

Hashing Cipher: It allows a fixed-length hash value is computed as per the plain text in order to make recovery of plaintexts nearly impossible. Hash functions are also used by many operating systems to encrypt passwords. Hash algorithms are typically used to provide a digital fingerprint of a file's contents. Often, it is used to ensure that the file has not been altered by an intruder or virus (Buchanan, Li, & Asif, 2018). The shortfall of traditional cryptosystem in term of memory capacity, energy consumption, and extensive computations led to the quest for lightweight cryptosystem as discuss in next subsection.

2.2 Public Key Cryptography

Public key cryptography known as asymmetric key cryptosystem. Two different keys are used for encryption and decryption, that is, a public key and secret key (Sehrawat & Gill, 2018). Sender and receiver have its own public and secret keys. One key is used for encryption and the other key is used for decryption. The secret key, is a private in nature. Public key used to announce to users. If a sender wants to transfer data to the receiver, it will encrypt the data by using the receiver’s public key. On the other end, the receiver will decrypt the data using its own secret key. There are many algorithms that are based on asymmetric or public key cryptosystem, such as RSA (Rivest-Shamir-Adleman), Diffie-Hellman and ECC (Elliptic Curve Cryptography) (Buchanan et al., 2018).

2.3 Lightweight Cryptography

This cryptographic algorithm was developed to be used by resources-constrained gadget for power and bandwidth efficiency (Al Salami et al., 2016). It combines three cryptosystem primitives including: symmetric cryptosystem, asymmetric cryptosystem and hash functions (Mustafa et al., 2018). The main strengths of this technique are in its ability to operate on embedded device; and provides security for constrained devices (Al Salami et al., 2016).

In addition, lightweight cryptographic schemes implementation can be done on hardware, software or both (Mustafa et al., 2018). There are numerous lightweight cryptosystems for devices such as sensors, RFID tags, contactless smart cards and healthcare devices (Majumdar & Dutta, 2020; Ogundokun et al., 2022). A complete layout of classes of lightweight cryptosystem algorithms are illustrated in Figure 1 (Pandurang, 2020).

In lightweight cryptosystem structures, there are several mathematical operations used such has substitution permutation network, Feistel network, and XOR network. These are explained as follows:

2.2.1: Substitution Permutation Networks (SPN)

SPN is a class of block cipher that involved mathematical operations. SPN comprises of permutation layer, substitution layer and key mixing (Sehrawat & Gill, 2018) as shown in Fig. 2. A substitution or confusion function provides confusion through well-established substitution confusion layer. This layer provides S-boxes in non-linear operation. In addition, S-boxes are generated in a pseudo-random fashion from a key (Tentu, 2020). A permutation layer has P-box, known as diffusion layer. It takes the output of all the S-box of one round, permutes the bits, and feeds them into the S-box of the next round. A good P-box has the properties that the output bit of any S-box is distributed to as many S-box input as possible (Sehrawat & Gill, 2018).

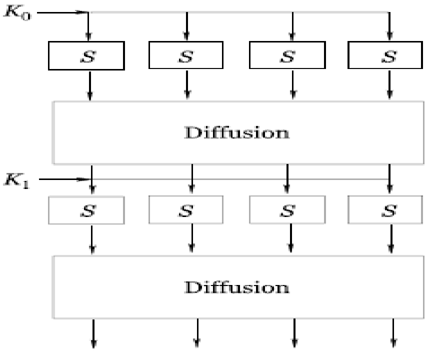

Figure 2. Substitution Permutation network (SPN) (Cusick & Stanica, 2017).

2.2.2: Feistel Networks

Feistel Networks (FNets) cipher is a symmetric structure used in the construction of block ciphers, FNets techniques operate on only half of the data per round and it requires more rounds compared to SPNs (Tentu, 2020). The FNets structure, as shown in Fig. 3, has the advantages that encryption and decryption operations are very similar, its requiring only a reversal of the key schedule. However, decryption process in the FNets type block cipher require high implementation cost, because FNets techniques use same program code for both encryption operations and decryption processes to reduce the memory requirements (Sehrawat & Gill, 2018).

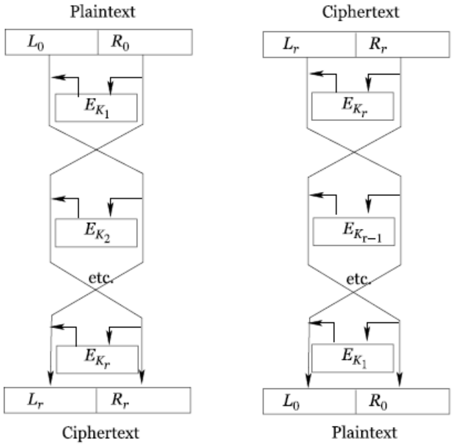

Figure 3. Encryption and Decryption in a Feistel Cipher with *r* round (Cusick & Stanica, 2017).

2.2.3: Exclusive OR Networks

The Exclusive OR (XOR) cipher is a type of an additive cipher in which encryption and decryption algorithms are performed. This structure basically a modulus 2 addition or subtraction which are identical. Single string of a text can be encrypted by applying the bitwise XOR operator to every single character using particular secret key as shown in Fig. 4. The XOR operator is major component of in complex cipher, it often adopted in computer malware to make reverse engineering more complex (Delfs, Paterson, & Cramer, 2015).

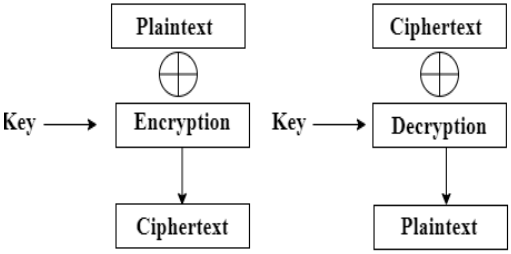

Figure 4. Encryption and Decryption in a XOR network Cipher.

3. Trends of Lightweight Cryptography in Smart Home Devices

Several studies have been carried out in the area of lightweight cryptosystem for smart home devices. SIMON block cipher cryptosystem paradigm was developed by Taware et al., (2020). It targeted m-commerce in other to provide maximum security for buying and selling of goods and services through wireless communication. This uses a meta-heuristic algorithm called Crow Search Algorithm (CSA) and cryptography parameters such as block size, key size and the number of rounds. The study used One-Hot Encode (OHE) techniques for reliability and security for encrypted key and gives maximum privacy preserving data in IoT. The drawback of this research is that it has 128-bit block size and 128 key size and 68 number of rounds, which leads to inefficiency of the system in terms of energy consumption.

A study by Toprak et al. (2020), developed a lightweight encryption algorithm for internet of things devices and medical sensors. This algorithm uses Shannon’s confusion and substitution principles. However, the S-box (substitution box) and p-box (permutation box) convert the block of input bits to corresponding output bits. Also, key scheduling was adopted in encryption and decryption, because the confidentiality of the data is totally dependent on the key and security-enhanced measurement should be considered in order to prevent access by an intruder. This algorithm makes use of two cipher structure which is substitution-permutation network and Feistel network, these two approaches make the cipher achieved maximum security. This is limited to integral cryptanalysis attacks and side-channel attack due to substitution permutation network adopted.

Moreover, the study in Raushan & Chaudhary (2020) came up with modified lightweight cryptographic technique for electronic-healthcare system. These techniques are based on Feistel network block cipher techniques. One Matrix Rotation, XOR and key expansion function were adopted. The encryption process mainly depends on key expansion function, round key generation function. MBCT made up of 256 bits Key size and 256-bit plain text has been consider for each round. There are 32 numbers rounds and after eighth round the intermediate cipher changes the bit structure by interchange left halve and right halve. The main strength of MBCT proposed method, it provides maximum security for e-healthcare system. The main drawback of this proposed method, it has high confusion and diffusion. As a result of complex relationship among encryption key and cipher text makes the block cipher inefficient, low throughput and high latency.

Similarly, Nozaki & Yoshikawa (2020) implemented unrolled prince cipher-based glitch physically unclonable function. It utilized a lightweight cipher circuit and prince block cipher was used and serves as glitch generator. Unrolled prince cipher-based glitch physically unclonable function target an unrolled architecture, which can extract glitch efficiently. Using glitch physically unclonable function, it provides a good performance, and resistance against modelling attacks. The main strength of Prince block cipher used in glitch PUF, it provides device's authentication and confidentiality of the system. The main weakness is the changes to the device temperature resulting in flip tendency when used at different temperatures, and a system situation called "weak cell".

Consequently, Dahiphale et al. (2020) were involved in design and implementation of various Datapath architectures for the ANU lightweight cipher on an FPGA. ANU is a balanced Feistel-based network, its supports 64-bit plaintext and 128/80-bit key length and it has 25 numbers of rounds. ANU uses two S-boxes in function F and bit permutation used to shuffle the bits and produce complexity in the block cipher. Proposed method implemented four different architectures with different data-path size, but the same data size and key size. ANU block ciphers have an essential component in the security analysis and produced a good avalanche effect and thus increase the randomness in respective bit positions. Limitation is the increase in the data path size in order to obtain more efficiency of the system. Also, it uses 128-bits key size and 64-bit data size which may require more energy.

Likewise, Mishra & Acharya (2020) developed high-throughput and low-area architectures of secure IoT algorithm for medical image encryption, the proposed method adopted Secure IoT (SIT) lightweight block cipher, SIT is an encryption algorithm that tends to consume small hardware resources due to simple operation, reduction of area and less power consumption. Finite State Machine model was used, because it required a lesser number of clock cycles for encryption. The main advantage of SIT for medical image encryption is to provide maximum security and resource utilization for constrained devices, also SIT pipelined architecture provides maximum degree of speed and higher throughput.

In the same vein, Shahbodin et al. (2019) worked on lightweight cryptography techniques for MHealth cybersecurity. MHealth system transmitting the patient's data in wireless instead of using personal computer or laptop for data collection. However, the encrypted sensor is used to collect data by mobile through Arduino software. The main strength of mobile health system is method of adopting encryption algorithms, because encryption algorithms are used for achieving security and confidentiality during information shearing. The main drawback of this proposed algorithms was inability of the encryption algorithms to faces many attacks like related key attacks, linear attacks and differential attacks.

High Throughput Lightweight Cryptographic Block Cipher Model for Low-Cost RFID Systems was developed by Anusha & Shastrimath (2019). This proposed method makes use of Extended Tiny Encryption Algorithm (XTEA), XTEA uses algebraic function includes shifting, addition and XOR with small operations code. The XTEA makes used of simple Feistel network structure with fastest and maximum efficient lightweight cryptosystem block cipher which is having 128-bit key size and 64-bit block size and 64 number of rounds. The main potency of XTEA is to improve TEA by correcting the key scheduling weakness by many attacks and enhance the security efficiency. The proposed XTEA makes use of 128-bit key size and has 64 number of rounds which may cause the system to consume excess power.

Additionally, Luo et al. (2016) developed a bright block cipher for IoT-enabled smart environment, the proposed method is a software oriented and the techniques of the proposed design gives fast diffusion. It is a family of lightweight block ciphers and it has a 4-branch generalized Feistel network that has comparably light round functions. However, the proposed method is deployed with two block sizes 64-bit and 128-bit as well as supportive of several key sizes such as 80, 96, 128, 192 and 256 bits. In addition, it makes use of key whitening, key whitening plays an important role in repelling some attacks.

Furthermore, Liu et al. (2019) developed an involutional lightweight block cipher (Loong). It is a new Substitution Permutation Network, which makes encryption and decryption have the same process. Having the same process, the number of rounds definitely reduces, and it can be shared for both software and hardware implementation. Loong has 64-bit block size with 64-bit to 128-bit key size. It has better diffusion and confusion implementation, and the diffusion realization as an effect than other lightweight block ciphers. However, having same encryption and decryption process can allow intruder to focus on one algorithm, breaking encryption algorithm, the decryption algorithm can be compromised since they share the same process.

Koo et al. (2018) introduced a lightweight block cipher for resource- constrained devices (CHAM), is based on Feistel network with ARX (Addition Rotation XOR) operations. It consists three based cipher, CHAM 64/128-bit, CHAM 128/128-bit, CHAM 128/256-bit, CHAM adopted a stateless-on-the-fly key scheduling which does not need for updating a key state. Fortunately, CHAM achieves outstanding performance on typical IoT platform and it shows a level of performance compared to SPECK lightweight. However, the block size and key size of this proposed methodology is higher, therefore it’s consumed more power compared to less lightweight parameters.

Relatedly, Roy et al. (2019) developed cellular automata-based encryption technique for IoT application, its method adopted a symmetric key encryption technique and encryption was deployed at the perception layer, where the sensing element are deployed and decryption algorithm was done at the network layer where the gateway of the networks is installed. Inessential, it handled the limitation of internet of things nodes deployed at the perception layer of the networks. In addition, the algorithm adopted are capable of implemented in pipeline programming paradigm, which make the system reduce the runtime. However, it has limitation of key management due to the adopted symmetric key encryption technique.

Also, Jebri et al. (2020) developed an enhanced lightweight algorithm to secure data transmission in IoT system, proposed algorithm used Elliptic Curve Cryptography, Identity Based Encryption and Pseudonym Based Cryptography. By integrating the dynamic virtual identities and the anonymity of link direction. Besides, AVISPA tools and BAN method are used to resists several attacks. The system able to fulfils security challenges in IoT application such as link direction anonymity, mutual authentication and sender/receiver anonymity, which gives trust between communication nodes. Limited to discussion on the efficiency of the system used on IoT devices.

While, Oluwade et al., (2021) developed an enhanced tiny encryption algorithm for secured smart home, The proposed methodology involves the Entropy Generation Technique (EGT) and access point and integration of modem on the development board (such as raspberry pi). Also, the smart home was developed using Raspberry pi3 as the access point for the smart home network. Thus, the system able to get rid of its weakness of predictable keys and vulnerabilities of possible related key attacks in smart home gadget through stretching, shifting and mixing technique. However, the system focused on only one attacks whereas there are many attacks threating IoT smart devices.

An enhanced energy efficient lightweight cryptography method for various IoT devices developed by Prakasam et al. (2021). The scheme adopted symmetric block ciphers by utilizing 8-bit manipulation, this cipher extensively depends on S-boxes (Substitution boxes) cryptography. Also, Multi-sequence Linear Feedback Shift Register (MLFSR) was used in order to reduce the area with optimal speed and less power consumption. MLFSR uses shift register, XOR operation and a shifting method operation to generate a sequence of binary states, also feedback the current state through direct computation. The shows improvements on power consumption and memory management due to low weight and security in nature. It can be also applied in real-time high secured applications such as time stamping, authentication system, electronic money transfer and so on. Though, the system was inability to verify and validate the speech in real- time applications.

Rawswami et al. (2021) developed a highly secured and geographic coordinate system based authenticated lightweight block cipher for smart system, the proposed scheme used Fibonacci series for the block cipher, it was designed base on substitution permutation network type cryptographic operation. This cipher reads the plaintext and transform it ciphertext using single key with multiple rounds. It attained some security objectives such as confidentiality, integrity and authentication mechanism by using different technique like cryptography operation, signature creation and signature verification. Unfortunately, the scheme has good security features but limited to efficiency and convenience due to series of stages smart home devices going through.

An Ultra-lightweight cryptographic scheme for IoTs was developed by Sleem & Couturier (2021). The proposed system is a hybrid block cipher by combining the Addition Rotation Exclusive OR (ARX) with a dynamic substitution layer. The Substitution boxes (S-Boxes) are established using a dynamic key and then varied according to the number of iterations, the system chose 64 bits block size and 96 bits key size for the algorithm. The main strength of the system is in the reduction number of rounds of entire algorithm from 26 to 7 while maintaining the aspect of security. The execution time of the drastically reduced due to decrement in number of rounds.

More so, Iqbal et al. (2021) improved on SDN enabled smart home by the used of privacy preserving communication schemes, the proposed system was based on three cryptographic lightweight technique such as key establishment, authentication and searchable encrypted user queries. In the system keys are distributed among the entity during the key establishment, likewise the authentication serves as a mutual parameter between the involved entities and the searchable index established on the shared private key between the user and smart device by the searchable encryption protocol. The system was able to integrate SDN into smart home device which allows the record the personal behaviors, encrypted the queries and secure data on the smart home. But, the time complexity of system was higher due extended processes leading to the inability to cater for efficiency and convenience.

Table 1 shows comparison of reviewed related works in the subject domain.

Table 1 Comparison of lightweight cryptographic schemes for smart home devices.

Author(s)	Schemes	Key Size (Bit)	Block Size (Bit)	Scope	Future Work
Taware et al. (2020)	SIMON-CSA (Crow Search Algorithm)	128	128	It consumes time, and inconvenience to operate.	To improve security by a Multi-Cloud Architecture.
Toprak et al. (2020)	Lightweight Encryption Algorithm (LWE)	64	64	It is unable to discover unknown attacks on medical sensor and IoT devices.	To enhance security to be able to identify known and unknown attacks.
Raushan & Chaudhary (2020)	Lightweight Ciphering Technique (LCT)	256	256	It is memory and time ineffective because of swapping XORing and splitting the data.	To implement linear crypto-analysis and differential for robustness.
Nozaki & Yoshikawa (2020)	Physically Unclonable Function Technique (PUFT)	128	64	It is less applicable for IoT devices security.	To secure IoT gadgets using PUFT.
Dahiphale et al. (2020)	ANU Datapath Architecture Algorithm	128/80	64	It is power-inefficient for IoT devices using different datapath architectures.	To extend operations for various datapath architectures, and reduce power consumption.
Mishra & Acharya (2020)	Serial and Pipelined Architecture Algorithm	64	64	It provides faster encryption, but less secure for IoT devices.	To provide lightweight blocks cipher for IoT security.
Sehrawat & Gill (2019)	BRIGHT Lightweight Block Cipher Algorithm	64	128	It provides security for IoT devices, but, inefficient due to large key sizes.	To improve performance, and conduct cryptanalysis.
Shahbodin et al. (2019)	Lightweight Cryptographic	Unspecified	Unspecified	Low security.	To improve on lightweight S-Box

	Protocols and Privacy Preserving Algorithms				design with variety of designs.
Anusha & Shastrimath (2019)	Extended Tiny Encryption Algorithm (TEA)	128	64	The performance lags and huge energy consumption, but, attained certain level of security,	To improve XTEA design compatible with RFID. To develop security protocol for low-cost IoT platform.
Girija & Manickam (2020)	PriPresent Lightweight Block Cipher Algorithm	128/80	64/80	It is unable to discovered attacks through offline networks. Huge block and key sizes.	To address both online and offline attacks recognition on IoT devices.
Sadhya & Mishra (2020)	Lightweight Addition-Rotation-XOR (LiARX) Block Cipher.	128	64	LiARX algorithm is limited to ARX-boxes with large inefficiency.	To increase the ARX-boxes for the better security.
Sleem & Raphael (2020)	An ultra-lightweight cryptography Algorithm (Speck-R)	96	64	It reduces the number of rounds, but, low throughput with large gate equivalent.	To obtain simpler execution times for both software and hardware components.
Al-ahdal et al. (2020)	NLBSIT Algorithm	64	64	It offers low security for IoT devices.	To focus on security enhancement and efficiency.
Sadhukhan, Ray, & Khan (2020)	Elliptic Curve Cryptography Based Algorithm	Unspecified	Unspecified	Symmetric keys and passwords are unsynchronized.	To target IoT networks.
Deebak (2020)	Lightweight Authentication and Key Management Algorithm	Unspecified	Unspecified	High throughput and transmission delay due to layers of authentication.	To test in a real-time environment.
Al-rahman (2018)	Low-Cost Encryption Algorithm	128/80	64	Repeated round function for better security. High inefficiency.	To minimize complex round function and key size for security of IoT.
Bansod, Pisharoty, & Patil (2018)	GRANULE Lightweight Block Cipher Algorithm	128/64	64	It offers low archive gate count, and large key sizes.	Unspecified.
Shantha & Arockiam (2018)	SAT_Jo Lightweight Block Cipher Algorithm	80	64	It is mostly applicable to tag-based application rather than IoT applications.	To deploy on different IoT platforms to efficiency of the system.
Luo et al. (2016)	Lightweight Authentication Protocol	Unspecified	Unspecified	Communication inaccuracy during authentication.	Unspecified

	Technique				
(Liu et al., 2019)	Substitutional Permutation Network Algorithm	128	64	Encryption and decryption process are the same. Intruder attacks are widespread.	To decouple encryption and decryption for security.
Koo et al. (2018)	Addition, Rotation and Exclusive OR Based Algorithm	64/128	128/256	The block size and key size are large causing power inefficiency.	To redesign lightweight parameters for the smart home devices
Roy et al. (2019)	Symmetric Key Encryption Technique	Unspecified	512	High key management due to single key adoption.	Designed a special resource-constrained for environments, thus it can scale up for a large number of sensor nodes.
Jebri et al. (2020)	Elliptic Curve Cryptography and Pseudonym Based Cryptography	Unspecified	Unspecified	Applicable to IoT devices.	Unspecified
Oluwade et al. (2021)	Entropy Generation Technique	128	64	It resists one attack on IoT smart devices	Entropy generation to be raised for better key generation and management.
Iqbal et al. (2020)	Anonymous Lightweight Authentication Mechanism (ALAM)	Unspecified	Unspecified	It is mostly applicable for privacy issues of smart ecosystem.	Searchable encrypted queries-based solutions with SDN as countermeasure for privacy attack and user profiling.
Ramaswami (2021)	FibGeoPresent algorithm	80/128	64/80	It provides good security features but limited to efficiency and convenience.	To extends the security goals (such as availability) for sharing of sensitive data.
Iqbal et al. (2021)	Privacy Preserving Communication Scheme (PPCS)	Unspecified	Unspecified	The time complexity of system is higher. It is unable to cater for efficiency and convenience.	To investigates Single Sign-One (SSO) mechanism for heterogeneous networks.
Sleem & Couturier (2021)	Addition/ Rotation/ XOR (ARX) Algorithm	96	64	Huge key size, delay execution time and low efficiency.	To improve execution times and efficiency.

From Table 1, most of the lightweight cryptography for IoT devices used larger block size and larger key size which leads to inefficiency and inconvenience on IoT smart device. Studies in Toprak et al. (2020), Raushan & Chaudhary (2020), Liu et al. (2019) and Girija & Manickam (2020) adopted substitution permutation network. Also, Sehrawat & Gill (2020); Shantha & Arockiam (2018); Shantha & Arockiam (2018) leveraged on Feistel network structure. While, Oluwade et al. (2021) used Raspberry pi development board to perform encryption on valuable data and securing smart appliances in homes.

Majority of smart homes systems favor substitution permutation network and Feistel network which lead huge block size and large key size; however, the mathematical computations of those networks required a huge memory space for constrained devices. XOR based cipher permit the lightweight block and key which suitable for IoT devices in terms of mathematical and logical efficient similar to optimization problems (Okewu et al., 2017; Crawford et al., 2020). But, in terms security SPN and Feistel are better. The proposed system design is shown in section 4 attempts to overcome the identified research gaps while strengthening the reviewed works.

4. Secure Smart Home System Architecture

The conceptual design of secure smart home system is composed of software and hardware subsystems as discussed as follows:

4.1 Software System Design

The proposed software system design is shown in Figure 5.

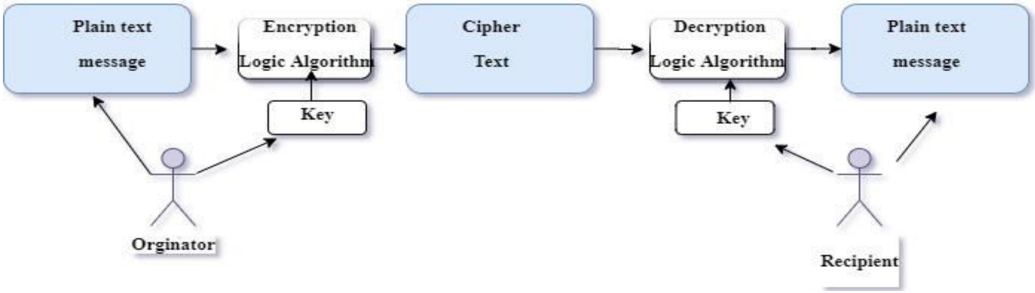

Figure 5. The proposed software system design.

The software architecture consists of three units: originator unit, transformation unit and recipient unit. The details of activities are presented as follows:

Originator unit: In this unit, user creates and send its private key and message to the receiver. Given more details, the key is use to encrypt the messages and transfer it into cipher text unit. At originated stage, it normally requires for private key size and message text size.

Transformation unit: This receives the message and converts it to an encrypted message using Ultra-Sooner lightweight cryptography. Actually, the originated and recipient are incapable of understanding the message in transformation unit. At this stage, is a cryptosystem stage, the messages have transformed to another form completely.

4.1 Hardware System Design

Figure 6 shows the basic electronic components to be used in this proposed scheme are Arduino Uno development board, Servo motor, Universal Serial Bus (USB) serial communication, power supply, laptop computer.

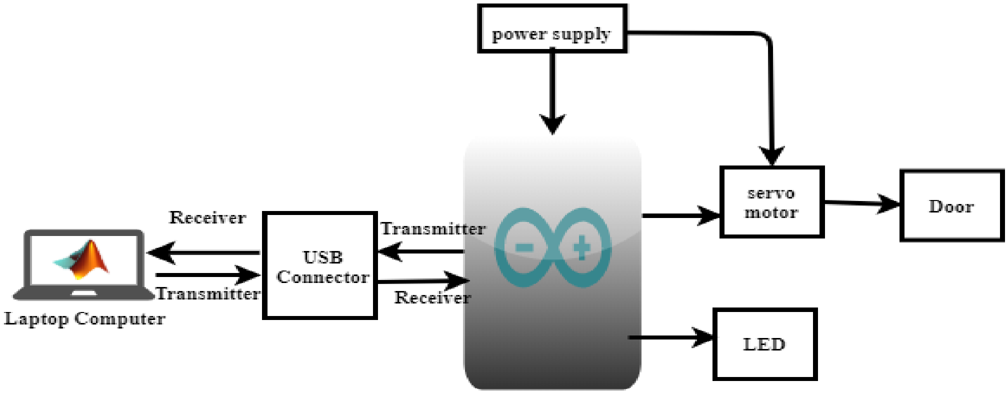

Figure 6. The block diagram of the Ultra-Sooner lightweight cryptosystem for Smart home door.

Laptop communication, servo motor connected to Arduino Uno board and makes the smart door open when the private key on encryption algorithms matches the secret key on decryption algorithms. The power supply unit is used as the source of power to Arduino Uno board and Arduino board power smart door. computer was programmed with Ultra-sooner lightweight cryptosystem algorithms and its bidirectional connected to Arduino uno board through universal serial bus serial. Also, the complete flow diagram of proposed Ultra-Sooner lightweight cryptosystem for smart home devices shows in Figure 7.

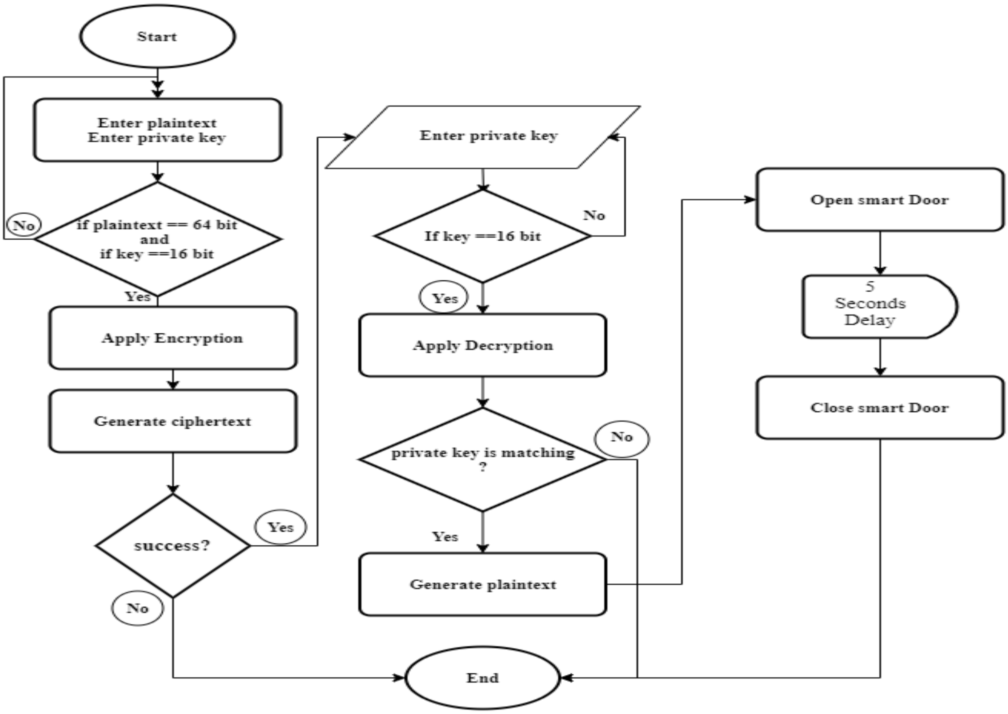

Figure 7. The complete Ultra-Sooner secured home door operational flow diagram.

5. Conclusion

This paper carried out a survey to examine the lightweight cryptosystem of smart devices. It highlights solution to efficiency and security issues of IoT devices. However, these solutions have been limited by: large block size, large key size, and complex rounds in cryptosystem. Therefore, Ultra-sooner lightweight cryptosystem for smart home devices has been proposed to mitigate these limitations. The next phase of this work is to fully implement the proposed cryptosystem in a smart door system to provide efficient, security, low-cost and less energy consumption data protection layer to SHT. In future, there is need to consider the blockchain-based lightweight cryptographic schemes for smart home devices for better security.

References

Al-ahdal AHA, Al-rummana GA, Shinde GN, Deshmukh NK (2020) NLBSIT: A New Lightweight Block Cipher Design for Securing Data in IoT Devices. Int. Journal of Computer Sciences and Engineering, 8(10).

Alfa, AA., Misra S, Attah BI, Ahmed KB, Oluranti J, Ahuja R (2022) Nigeria Human Population Management Using Genetic Algorithm Double Optimized Fuzzy Analytics Engine Approach. Lecture Notes in Electrical Engineering (pp. 203–215).

Al-rahman SQA (2018) NVLC: New Variant Lightweight Cryptography Algorithm for Internet of Things. In 2018 1st Annual Int. Conference on Information and Sciences (AiCIS) (pp. 176-181). IEEE.

Al Salami S, Baek J, Salah K, Damiani E (2016) Lightweight encryption for smart home. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 382-388). IEEE.

Anusha R, Shastrimath VVD (2019) LCBC-XTEA: High Throughput Lightweight Cryptographic Block Cipher Model for Low-Cost RFID Systems. In Computer Science Online Conference (pp. 185-196). Springer, Cham.

Balas VE, Kumar R, Srivastava R (Eds.) (2020) Recent Trends and Advances in Artificial Intelligence and Internet of Things (pp. 389-425). Springer.

Bansod G, Pisharoty N, Patil A (2018) GRANULE: an ultra lightweight cipher design for embedded security. Cryptology ePrint Archive.

Buchanan WJ, Li S, Asif R (2018) Lightweight cryptography methods. Journal of Cyber Security Technology 1(3-4), 187-201.

Chaoyun L (2020) New Methods for Symmetric Cryptography.

Cusick T, Stanica P (2017) Cryptographic Boolean Functions and Applications (2nd edition). Academic Press.

Crawford B, Soto R, Palma W, Aballay F, Lemus-Romani J, Misra S, Rubio JM (2020) A Teaching-Learning-Based Optimization Algorithm for the Weighted Set-Covering Problem. Tehnički Vjesnik, 27(5), 1678-1684.

Dahiphale V, Bansod G, Zambare A, Pisharoty N (2020) Design and implementation of various datapath architectures for the ANU lightweight cipher on an FPGA. Frontiers of Information Technology & Electronic Engineering, 21(4), 615–628.

Deebak B D (2020) Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. Sustainable Cities and Society, 63, 102416. https://doi.org/10.1016/j.scs.2020.102416

Delfs H, Paterson K, Cramer R (2015) Introduction to Cryptography (vol. 2). Heodelberg: Springer.

Fakroon M, Alshahrani M, Gebali F, Traore I (2020) Internet of Things Secure remote anonymous user authentication scheme for smart home environment. Internet of Things, 9, 100158.

Girija M, Manickam P (2020) PriPresent: an embedded prime LightWeight block cipher for smart devices. Peer-to-Peer Networking and Applications, 14(4), 2462-2472.

Iqbal W, Abbas H, Deng P, Wan J, Rauf B, Abbas Y, Rashid I (2020) ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes. IEEE Internet of Things Journal, 8(12), 9622-9633.

Iqbal W, Abbas H, Rauf B, Abbas Y, Amjad F, Hemani A (2021) PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes. IEEE Sensors Journal, 22(18), 17677-17690.

Jebri S, Ben A, Mohamed A, Ammar A (2020) Enhanced Lightweight Algorithm to Secure Data Transmission in IoT Systems. Wireless Personal Communications, 116(3), 2321-2344.

Koo B, Roh D, Kim H, Jung Y, Lee DG, Kwon D (2018) CHAM: A family of lightweight block ciphers for resource-constrained devices. In International conference on information security and cryptology (pp. 3-25). Springer, Cham.

Liu BT, Li L, Wu RX, Xie MM, Li QP (2019) Loong: A family of involutional lightweight block cipher based on spn structure. IEEE Access, 7, 136023–136035.

Luo H. Wen G, Su J, Huang Z (2016) SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system. Wireless Networks, 24(1), 69-78.

Majumdar ABA, Dutta SNA (2020) LRBC: a lightweight block cipher design for resource constrained IoT devices. Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-01694-9

Mishra Z, Acharya B (2020) High throughput and low area architectures of secure IoT algorithm for medical image encryption. Journal of Information Security and Applications, 53, 102533. https://doi.org/10.1016/j.jisa.2020.102533

Misra S (2021) A Step by Step Guide for Choosing Project Topics and Writing Research Papers in ICT Related Disciplines. Communications in Computer and Information Science (CCIS) (vol. 1350). Springer.

Mustafa G, Ashraf R, Mirza MA, Jamil A, Muhammad A (2018) A review of data security and cryptographic techniques in IoT based devices. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (pp. 1-9) https://doi.org/10.1145/3231053.3231100

Nozaki Y, Yoshikawa M (2020) Unrolled PRINCE Cipher based Glitch Physically Unclonable Function. In Proceedings of the 2020 3rd Internal Conference on inforamtion Science and System (pp. 3–7).

Ogundokun R O, Misra S, D, Damaševičius R, Maskeliunas R (2022) Medical Internet-of-Things Based Breast Cancer Diagnosis Using Hyperparameter-Optimized Neural Networks. Future Internet, 14 (5), https://doi.org/10.3390/fi14050153

Ogundokun RO, Maskeliunas R, Misra S, Damaševičius R (2022) Improved CNN Based on Batch Normalization and Adam Optimizer. Lecture Notes in Computer Science (LNCS) (pp. 593–604).

Okewu E, Misra S, Maskeliūnas R, Damaševičius R, Fernandez-Sanz L (2017) Optimizing Green Computing Awareness for Environmental Sustainability and Economic Security as a Stochastic Optimization Problem. Sustainability, 9, 1857.

Oluwade OR, Olaniyi OM, Simpa Y, Ajao LA, Osang FB (2021) ETEASH - An Enhanced Tiny Encryption Algorithm for Secured Smart Home. Covenant University of Informatics and Communication Technology, 9(1).

Padhye S, Saraswat V (2018) Introduction to Cryptography. CRC Press.

Pandurang JS (2020) Towards Light Weight Cryptography Schemes for Resource Constraint Devices in IoT. Journal of Mobile Multimedia, 91-110.

Prakasam P, Madheswaran M, Sujith KP, Sayeed S (2021) An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices. ICT Express, https://doi.org/10.1016/j.icte.2021.03.007.

Yoshizawa T, Preneel B (2019) Survey of security aspect of v2x standards and related issues. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 1-5). IEEE.

Rana N, Abd Latiff MS, Misra S (2021) A hybrid whale optimization algorithm with differential evolution optimization for multi-objective virtual machine scheduling in cloud computing. Engineering Optimization, https://www.tandfonline.com/doi/full/10.1080/0305215X.2021.1969560

Ramaswami MGPMM (2021) FibGeoPresent: A Highly Secured and Geographic Coordinate System Based Authenticated Lightweight Block Cipher for Smart System. Wireless Personal Communications, 1-18. https://doi.org/10.1007/s11277-021-08783-8

Raushan R, Chaudhary K (2020) An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System. In 2020 5th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 991–

995). IEEE.

Roy S, Rawat U, Karjee J (2019) Encryption Technique for IoT Applications. IEEE Access, 7, 39782-39793.

Sadhukhan D, Ray S, Khan GPBMK (2020) A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. In The Journal of Supercomputing, 77(2), 1114-1151.

Sadhya D, Mishra S (2020) LiARX: A Lightweight Cipher Based on the LTS Design Strategy of ARX. In International Conference on Information Systtems Security (pp. 185-197). Springer, Cham.

Sarker VK, Gia TN, Tenhunen H, Westerlund T (2018) Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. In 2020 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

Sehrawat D, Gill NS (2018) Lightweight Block Ciphers for IoT based applications: A Review. International Journal of Applied Engineering, 13(5), 2258–2270.

Sehrawat D, Gill NS (2019) Bright - Proposed Family of Lightweight Block Ciphers for IoT-Enabled Smart Environment. International Journal of Innovative Technology and Exploring Engineering, 8(9), 584–592.

Sehrawat D, Gill NS (2020) Design Considerations of Lightweight Block Ciphers for Low-Cost Embedded Devices. International Journal of Recent Technology and Engineering, 8(2), https://doi.org/10.35940/ijrte.A2140.078219

Shahbodin F, Ali T, Ku C, Che N, Mohd K (2019) Lightweight Cryptography Techniques for MHealth Cybersecurity. In Proceedings of the 2019 Asia Pacific Information Technology Conference (pp. 44-50).

Shantha MJR, Arockiam L (2018) SAT_Jo: An enhanced Lightweight Block Cipher for the Internet of Things. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1146–1150). IEEE.

Sharma TP (2020) Lightweight encryption algorithms, technologies, and architectures in Internet of Things. In Innovations in Computer Science and Engineering (pp.341-351). Springer, Singapore.

Shouran Z, Ashari A, Priyambodo T (2019) Internet of Things (IoT) of Smart Home: Privacy and Security. International Journal of Computer Applications, 182(39), 3-8.

Sleem L, Couturier R (2021) Speck-R: An Ultra Light-Weight Cryptographic Scheme for Internet of Things. Multimedia Tools and Applications, 80(11), 17067-17102.

Sovacool BK, Rio DDF (2020) Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. Renewable and Sustainable Energy Reviews, 120, 109663. https://doi.org/10.1016/j.rser.2019.109663

Taware S, Chakravarthi RR, Palagan C A, Chandrasekaran K (2020) Preserving mobile commerce IoT data using light weight SIMON block cipher cryptographic paradigm. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6081-6089.

Tentu AN (2020) A Review on Evolution of Symmetric Key Block Ciphers and Their Applications A Review on Evolution of Symmetric Key Block Ciphers and Their Applications. IETE Journal of Education, 61(1), 34-46

Thangamani N, Murugappan M (2019) A Lightweight Cryptography Technique with Random Pattern Generation. Wireless Personal Communications. Wireless Personal Communications, 104(4), 1409-1432.

Toprak S, Akbulut A, Aydın MA, Zaim AH (2020) LWE: An Energy-Efficient Lightweight Encryption Algorithm for Medical Sensors and IoT Devices. Electrica, 20(1), 71-80.

Zaidan AA, Zaidan BB (2020) A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artificial Intelligence Review, 53(1), 141-165.