J Ambient Intell Human Comput (2024) 15:1625–1642
DOI 10.1007/s12652-017-0494-4

ORIGINAL RESEARCH

Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions

Saurabh Singh[1] · Pradip Kumar Sharma[1] · Seo Yeon Moon[1] · Jong Hyuk Park[1]

Received: 29 January 2017 / Accepted: 18 April 2017 / Published online: 24 May 2017

Abstract There are many emerging areas in which highly constrained devices are interconnected and communicated to accomplish some tasks. Nowadays, Internet of Things (IoT) enables many low resources and constrained devices to communicate, compute process and make decision in the communication network. In the heterogeneous environments for IoT, there are many challenges and issues like power consumption of devices, limited battery, memory space, performance cost, and security in the Information Communication Technology (ICT) network. In this paper, we discuss a state-of-art of lightweight cryptographic primitives which include lightweight block ciphers, hash function, stream ciphers, high performance system, and low resources device for IoT environment in details. We analyze many lightweight cryptographic algorithms based on their key size, block size, number of rounds, and structures. In addition, we discuss the security architecture in IoT for constrained device environment, and focus on research challenges, issues and solutions. Finally, a proposed security scheme with a service scenario for an improvement of resource constrained IoT environment and open issues are discussed.

Keywords Lightweight cryptography · Symmetric algorithms · Constrained devices · Internet-of-things

1 Introduction

Internet of Things (IoT) is a novel worldview that is quickly making progress in the field of cutting-edge remote media communication. IoT is a global movement that unites people, data, processes, and things to build network connections that are more pertinent and useful than ever before. It is a system of interrelated computing items, such as RFID tags, sensors, actuators, and cell phones; digital machines; and people that provides the ability to transfer data over a network without requiring human-to-computer or human-to-human interactions.

According to the Gartner report (Stamford 2013) IoT, which exclude PCs, tablets, and smartphones, will generate more than $300 billion in revenue until 2020. Furthermore, the number of smartphones and tablets will reach up to 7.3 billion units by 2020. These devices will create a huge and complex network where a massive amount of data is communicated throughout the network. As IoT is growing rapidly, it faces risks and challenges, such as how to handle huge amounts of data, processing power deal with energy consumption, address security threats, and how to encrypt/decrypt of huge data.

To address these challenges when many smart devices are connected in an IoT environment, the increasing demand for the use of appropriate cryptographic solution into the embedded applications. However, these smart devices generally have constrained resources or they can be called low-resource devices in regards to their low computation power, limited battery life, small size, small memory, and limited power supply. Hence,

✉ Jong Hyuk Park
jhpark1@seoultech.ac.kr

Saurabh Singh
singh1989@seoultech.ac.kr

Pradip Kumar Sharma
pradip@seoultech.ac.kr

Seo Yeon Moon
moon.sy0621@seoultech.ac.kr

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 139-743, South Korea

the conventional cryptographic primitives might not be suited for low-resource smart devices. For example, the 1204-bit RSA algorithm (Padmavathi and Kumari 2013) cannot be implemented in RFID tags. Moreover, the tight constrains inherent the mass developments of smart devices that impeding the requirements of developing a new cryptographic algorithm, which performs strong security mechanism, encryption/decryption, with low power applications and other functionalities for the pervasive computing. This new research area is referred as lightweight cryptography.

The two main reasons for adopting new technology for IoT are listed below.

Efficiency of end-to-end communications To apply the lightweight symmetry key algorithm in order to achieve end-to-end security and with lower power consumption in the low resources devices.

Adoptability in low resources smart devices Lightweight cryptography's footprints are much smaller than classical ones. It has the possibilities of more network connection with lower resource smart devices.

According to NIST, lightweight cryptography is a subcategory of cryptography that aims to provide solutions for rapidly growing applications that broadly employ smart low power constrained devices (McKay et al. 2016). It targets a wide variety of devices that might be realized on hardware/software. A conventional cryptographic algorithm may perform well in computers, servers, and some mobile phones. But on the other hand, the lower ends of spectrum are devices like RFID tags, sensing devices and sensor networks, and embedded system. These devices and networks require lightweight cryptography platforms.

The applications for the lightweight cryptography algorithm include the Wireless Sensor Network (WSN) (Yick et al. 2008) RFID, Wireless Body Area Network (WBAN) (Latré et al. 2011) IoT, smart cards, etc.

IoT supports creating connections and building networks between dissimilar objects or devices in the heterogeneous environment. In IoT, devices are communication without or very less human interventions. The unconnected entities, like barcodes, can also become part of data communicating devices. IoT has also exposed many security attacks as well as any device can unauthorized access to the network and damage the network connection. This leads to the security parameters and network privacy being compromised. In addition, IoT utilizes the cloud computing concept, which has many security issues and challenges (Sajid et al. 2016; Singh et al. 2016a, b, c; Kar and Mishra 2016; Zhou et al. 2017). Apart from these issues, the resource-constrained devices, which have less computation power, limited battery life, a small amount of memory, and low bandwidth, so an efficient security solution is being required that will not crunch the resources of IoT.

The rest of this paper is comprised as follows: In Sect. 2, the lightweight cryptographic primitives are discussed. Section 3 discusses security challenges and counter-measures in IoT. In Sect. 4, we discuss and propose an idea. Finally, we conclude our research in Sect. 5.

2 Lightweight cryptographic primitives

In this chapter, we discuss the different primitives of lightweight cryptographic algorithms as shown in Fig. 1 and also, we summarize many lightweight algorithms in the Table 1 based on their key size, block length, number of rounds and structures.

2.1 Lightweight block ciphers

Xinxin Fan et al.'s research (Fan et al. 2013) presented a lightweight cipher WG-8 as a cryptographic algorithm, which is tailored from the Welch-gong cipher family for low-resource devices. A number of block ciphers have been proposed in existing research to achieve better performance for items such as AES-128 (Iokibe et al. 2014), RC-5 (Rivest 1994), TEA Wheeler and Needham (1994) and XTEA (Yu et al. 2011). Generally, some of these were improved and designed by simplifying conventional block ciphers to improve their performance.

For an instance, DESL (Leander et al. 2007), which is also known as DES light weighted, which is a variant of classical DES (Saputra et al. 2003). In DESL, the round function uses a single S-box rather than repeat eight rounds, which results in the creation of initial and final permutation to increase hardware implementation. SIMON and SPECK (Beaulieu et al. 2015), which are from block ciphers, come in a variety of width and key sizes. Both are flexible with given platforms and perform well across the full spectrum of lightweight applications. Some of the lightweight block ciphers are explained in (du Luxembourg 2017).

Smaller block sizes In order to realize the performance benefits of lightweight block ciphers and to save money, the block size should be small. It should be less than AES at 64-bits instead of 128-bits. When the block size decreases, it limits the size of plain text.

Smaller key size In order to achieve power consumption with limited battery life, the key size must be small in a lightweight block cipher. For example, PRESENT (Bogdanov et al. 2007) is 80-bits in key size, and Twine (Hosseinzadeh and Hosseinzadeh 2016) is 80/128-bits in key size.

Simpler rounds Lightweight block ciphers that target low-resource constrained devices naturally have simple computation operations as compared with conventional block cipher algorithms. The number of rounds should be limited in lightweight design algorithms. For example, for

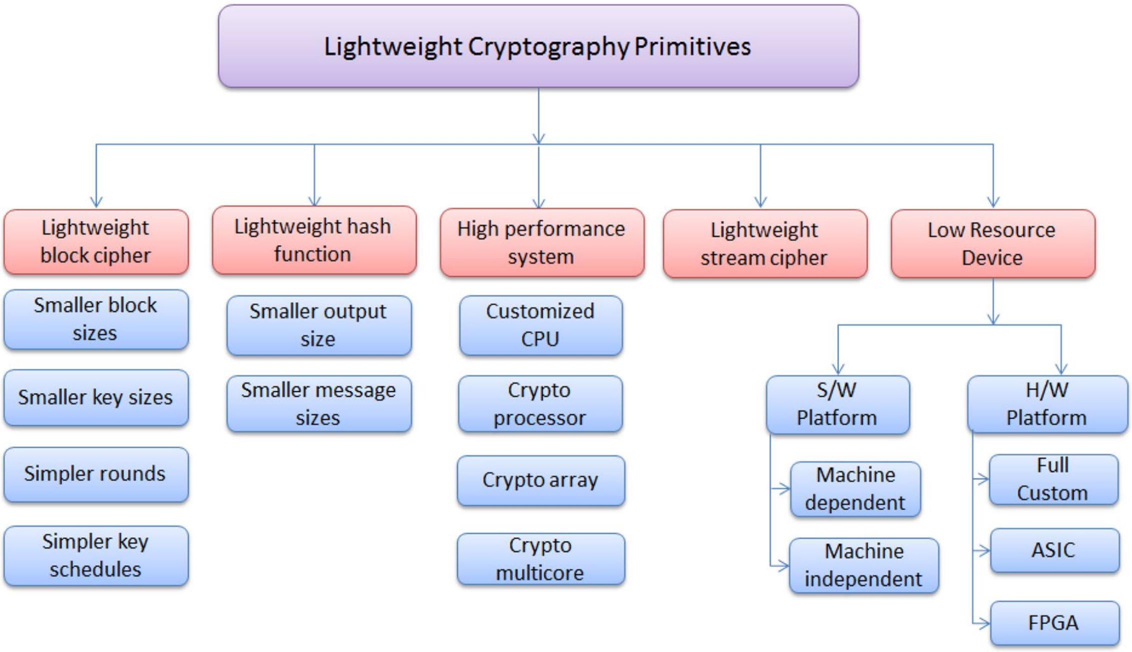

Fig. 1 Lightweight cryptographic primitives

Table 1 Summary of some lightweight cryptographic algorithms

Algorithm	Key size	Block size	Structure	No. of rounds
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
RC5	0–2040	32/64/128	Feistel	1–255
TEA	128	64	Feistel	64
XTEA	128	64	Feistel	64
LEA	128,192,256	128	Feistel	24/28/32
DES	54	64	Feistel	16
Seed	128	128	Feistel	16
Twine	80/128	64	Feistel	32
DESL	54	64	Feistel	16
3DES	56/112/168	64	Feistel	48
Hummingbird	256	16	SPN	4
Hummingbird2	256	16	SPN	4
Iceberg	128	64	SPN	16
Pride	128	64	SPN	20

a single S-box 4-bit S-boxes have been used in lightweight instead of 8-bit boxes in conventional cryptography. Some simpler lightweight cryptography algorithms are as follows: PRESENT uses 4-bit S-boxes, and Hummingbird2 (Mohd et al. 2015a) and Iceberg (Standaert et al. 2004) have only four rounds.

Simpler key schedules For a given key, a key schedule is a kind of algorithm that calculates the sub keys for rounds. Complex keys consume more memory and energy for their implementations. As such, a lightweight block cipher utilizes simpler key schedules, which can generate sub keys. For example, the block cipher of TEA simply splits a 128-bit key into four 32-bit keys.

2.2 Lightweight hash functions

In 2006, Feldhofer and Rechberger brought up the absence of using lightweight hash function in RFID protocols (Feldhofer and Rechberger 2006). A conventional hash function has a large internal state size and high power consumption, which may not be preferred for resource-constrained devices. Therefore, a lightweight has function in 2008 by Andrey Bogdanov et al. is presented which based on light weight block ciphers (Bogdanov et al. 2008). Some lightweight hash functions are PHOTON (Guo et al. 2011), Quark (Aumasson et al. 2013), SPONGENT (Bogdanov et al. 2011), and Lesamnta-LW (Hirose et al. 2010).

Smaller output size The vast amount of size is critical for applications that require hash-function collision resistance. For applications where collision resistance is not required, interior and balance sizes may be utilized. At the point where collision safe hash capacity is needed, this hash task should have similar security against pre-image, second image and impact attack. This can reduce the range of internal state.

Smaller message size Traditional hash capacity is used to reinforce the contribution of the huge size of roughly

264 bits. For the majority of objective rules on the capacity of lightweight hash, the regular information size is much lesser (like as at most 256 bits). In this way, hash functions that are enhanced for short messages may in this manner be more reasonable for lightweight applications.

2.3 High performance system

The elite system utilizes particular crypto motors to meet three essential necessities: throughput, adaptability, and security. Other constraints, such as area and power, are considered to a lesser degree (Bossuet et al. 2013). Next, we will discuss some of the requirements for achieving a high-performance system.

Customized CPU Cryptographic processors, such as CPU and Crypto ALU, utilize a CPU that has been optimized to execute the encryption algorithm. Normally, Instruction Set Architecture (ISA) integrates cryptographically-oriented instructions. The choice of these types of instructions is difficult due to the variety of encryption algorithms. In order to use a new instruction, the system program must be updated to something like compiler. Such kind of processor is the work of (Tillich and Großschädl 2006).

Crypto co-processor The upgrading of the encryption speed is accomplished by the equipment module, which is devoted to the encryption co-processor, the encryption business, and is controlled by the host processor. The handling of overhead information to and from the c-processor affects the general execution of data. Hodjat Alireza et al. have shown the co-processor case for DES and AES (Hodjat and Verbauwhede 2004).

Crypto array A cryptographic array of processing elements and a multicore cryptographic processor were developed by utilizing parallel computations for further improving the performance. Cryptographic arrays are close to algorithmic tasks and require a routing topology to move data between processing elements and memory.

Crypto multi-core On the other hand, the multi-core cryptographic processor does not depend on an algorithm. It delivers a highly-encrypted data rate or simultaneous use of different ciphers. Researchers (Grand et al. 2011) have announced an 8-core cryptographic processor (MCCP) configurable for multi-channel and multi-standard systems. The core implemented AES encryption on the FPGA platform. By reconfiguring the FPGA hardware, the AES core can be easily replaced with other block ciphers.

2.4 Lightweight stream ciphers

Stream ciphers are also encouraging primitives for obliged situations. The eSTREAM rivalry (ECRYPT 2017) sorted out by the European Network of Excellence for Cryptology, was set up for recognizing new stream figures that may be appropriate for boundless adoption. Competition finalists were announced in 2008 and included the three stream ciphers of Grain (Hell et al. 2007), MICKEY (Babbage and Dodd 2008) and Trivium (Kitsos et al. 2013) for hardware applications with limited resources.

2.5 Low resource devices and performance metrics

In the lightweight cryptographic algorithm, while considering the performance metrics in low-resource devices, there is an interpose between performance and resource to reach the same security levels. Performance can be conveyed in terms of power consumption, waiting time or latency, and throughput. In this section, there are two categories for cipher implementation in low-resource devices, which are as described below.

Software specific implementation and metrics The implementation of software was accomplished by running a cryptographic code on the processor. The code may be machine dependent (assembly) or independent (java). For example, if the code is written in C language, it may be implemented in a specific processor. Generally, a system works with 8- or 16-bits of low-cost microcontrollers. For a low constrain device, software implementations are focused on the amount of power, speed, and memory used. The software-specific metrics focus on the required number of register in RAM, and ROM.

Hardware specific implementation and metrics The resources required for hardware design and implementation are generally expressed in terms of gate area and use full custom ASIC, or FPGA. In FPGA, the design provides benefits like minimizing the development costs and increasing flexibility. It contains look-up tables, flip-flops, and multiplexers (Souissi and Ben-Ammar 2014). On the other hand, the customized design of ASIC is based on automated design flow to decrease the design time.

2.6 Existing researches

James and Kumar proposed a technique to implement AES as a lightweight block cipher in immediate requirement of time. They aim to develop AES into a lightweight block cipher by taking parameters latency and power as taking into considerations. Their proposed technique is applicable in sensor nodes and RFID tags (James and Kumar 2016).

Li et al. proposed an ultra-lightweight block cipher named QTL. The structure of QTL is basically a variation of the Feistel network structure for improving the slow diffusion of the traditional Feistel structure. In QTL, the encryption and decryption processes are the same. In addition, QTL occupies less area in a constrained application, and it reduces the cost of power consumption during hardware implementations (Li et al. 2016).

Karakoç et al. developed AKF, a key-altering Feistel scheme, which protects the cipher against related key attacks. Since a Feistel cipher without a key schedule is vulnerable to this type of attack, it focuses on the main attacks launched against it. They showed that by using the AKF scheme, it is easy to construct secure ciphers against related major attacks (Karakoç et al. 2015).

A new lightweight encryption algorithm design for embedded security was proposed by (Bansod et al. 2015). Their paper included an outline of another lightweight compact cipher system that is based on bit substitution instruction group operation, which has been studied extensively. By using the S-boxes of PRESENT, we include confusion part because all existing algorithms use bits permutation commands do not have the nature of this confusion. The existing S-boxes of compact algorithm and in this paper, a new hybrid system has been proposed which provides more compact results in terms of both memory spaces gate equivalent.

Biswas et al. surveyed numerous proposed security mechanisms, such as AES, LED, KATAN, and TWINE, for sensor networks to be able to achieve data confidentiality. However, these security mechanisms have drawbacks, security vulnerabilities, and high computational complexities. They addressed these challenges and proposed lightweight block ciphers using chaotic maps and genetic operations. Their proposed scheme utilizes points on an elliptic curve to identify the communicating nodes (Biswas et al. 2015).

Guo et al. proposed a framework that provides security and privacy protection combined with multilevel trust management. This scheme can rapidly accumulate processing force and capabilities in order to register large amounts of PHIs (individual health data) while limiting protection divulgence in medical service emergencies (Guo et al. 2015).

A tool for lightweight cryptography in the android platform was developed by Shushma Verma et al. They developed the user-friendly tool of NCRYPT for this platform. This tool helps to secure data when it is on rest. NCRYPT provides the options to encrypt all of the data or selected sensitive files. This property helps the efficiency of the tool (Verma et al. 2014).

Chunyan Peng et al. introduced an ultra-lightweight encryption scheme to tackle the problem of Underwater Acoust Networks (UANs). The S box of existing block cipher the algorithm is energy intensive do you mean something about it using or requiring a lot of energy or power to operate? and not suitable for resource-constrained UANs. In this paper, instead of S-box, lightweight eight round iterative block cipher algorithm for UAN communication based on chaos theory. This scheme can protect against brute force attacks and adversary attacks (Peng et al. 2016).

For pervasive computing, an ultra-lightweight encryption design has been suggested by Bansod et al. Their proposed ultra-lightweight cipher, ANU, consists of 25 rounds and supports 80/128-bit key scheduling (Bansod et al. 2016). ANU ciphers resist basic and advanced attacks, like MITM, Zeroday, and Biclique.

Buja et al. explained the direction of lightweight ciphers in the distributed cloud system, which we refer to as mobile big data computing. Their paper covers how to keep stored and transmitted data secure cryptography should works well with restricted resources for protecting information from attacks, such as information being changed by unauthorized users (Buja and Latip 2015).

3 Security challenges and countermeasures for IoT

3.1 Security architecture for IoT

Physical/perception layer IoT is a combination of a physical layer and a MAC layer Internet architecture. It is used to gather data by using RFID, sensors, or GPRS. In this layer, the IEEE 802.15.4. is used as a specification of IoT. IEEE 802.15.4 is a low cost, battery powered. It is an accessible security solution that still needs to address some of its existing loopholes against threats.

Network layer This is the second layer from the bottom that collects the data from physical layer. This layer is utilized to partition the message into bundles and to rout the parcels from source to goal by utilizing the IPv6 addressing instrument. As the IoT network rapidly increases the IPv4 address space takes precedence over IPv6 with more address spaces. Inbuilt cryptography conventions, like AES and DES, can be actualized by utilizing IPsec at this layer.

Transport layer For end-to-end communication, IoT utilizes the User Datagram Protocol (UDP). Since UDP is an unreliable protocol, a security mechanism using DTLS is built into this layer.

Application layer This is the upper most layer in which the actual development of IoT's intelligence is comprehended. The application layer can be the part of number of uses, such as for retail, social action, wellbeing, or individual needs. The Constrained Application Protocol (CoAP) (Shelby et al. 2014) has been utilized for low-resource constrained IoT devices and networks.

3.2 Research challenges and issues

3.2.1 Challenges

The key challenge of ubiquitous deployment is coordinating multi-innovation networks into a typical all-IP system to guarantee that correspondence systems have unwavering quality and versatility. For this reason, IoT depends on the availability and reliability of the correspondence on the future internet engineering and the IPv6 convention that meet the prerequisites of tending to and versatility.

The second challenge is to guaranteeing security, protection, data trustworthiness, and user confidentiality. Moreover, important and major IoT applications challenge for the mechanism that performs authentication, authorization, access control, and key management. Furthermore, as the abilities of compelled devices that can interface with the Internet are debased, it is important to fortify the protection of edge systems for global network.

Some more challenges are allied to IoT system which is as follows:

- Fewer human interventions may result in physical and logical attacks.
- Many researches already explored on the security vulnerabilities in IoT wireless sensor networks results many attacks like DoS/DDoS, reply attack, eves dropping, and many more.
- Another challenge is related to resources constrained devices in terms of power consumption, limited battery life, bandwidth, heterogeneous platforms, and intricate security methodologies that can delay the efficiency of device.

3.2.2 Issues

At present, IoT is recognized in families, workplaces, social facilities, business companies, etc. who face security and privacy issues. Therefore, security and privacy issues are the main reasons for concerning in the operation of IoT. Conventional cryptography algorithms do not fit perfectly in IoT scenario because of numerous resource limitations and conditions such as power, limited battery, and real-time execution and so on. Therefore, lightweight cryptography is more compatible to work with IoT environment. There are number of lightweight cryptographic algorithms that already exist in the research categories of symmetry and asymmetry algorithm, but these lightweight algorithm still do not give guarantee of security in real-time, execution time, power consumption and memory requirements. Symmetric algorithms lacks of authentication whereas asymmetric suffers its larger key size and the consumptions of more memory. This affects real-time information gathering and processing, and it wastes IoT resources.

3.3 Solutions and countermeasures for IoT

3.3.1 Symmetric lightweight algorithm for IoT

Advanced encryption standard (AES) According to NIST, AES has three versions of Rijndael cipher, which are AES-128, AES-192 and AES-256. It is used in the application layer by providing a solution in CoAP. The encryption operation consists of 4×4 matrix that has 128 bit sized blocks. The internal state is organized by subbyte, shiftrows, mixcoloumn, and addroundkey.

TWINE This utilizes Feistel structure which called 8 times per round and XOR operation on sub key and apply 4×4 S-box. Unlike CLEFIA and HIGHT, TWINE is more complicated permutation and combination to speed up diffusion. In TWINE, permutation only requires only half as many as rounds as the circular shift for single sub block difference to diffuse all sub-blocks.

High security and lightweight (HIGHT) Height utilizes very simple and basic operation to work for Feistel network. That key is generated during the encryption and decryption phases. Lee et al. proposed a parallel implementation which necessitate less energy, limited number of line of code, and improve the RFID system (Lee and Lim 2014). HIGHT has saturation attack vulnerability.

PRESENT This depends on SP-network and consists of 31 rounds. PRESENT is utilized as lightweight algorithm for security. It has a block length of 64 bits and two keys of 80 and 128 bits. For hardware implementation, it applied on substitution layer that utilizes 4-bits of input and the S-box output.

3.3.2 Asymmetric lightweight algorithms for IoT

RSA Generally, RSA does not belong to the lightweight cryptography system because of its large key size. Due to using two large prime numbers and performing modulo operation, RSA provides more security and maintains the privacy of users.

Elliptic curve cryptography (ECC) Compared to the RSA algorithm, ECC requires a smaller key size. As such, it has a fast processing speed and requires less memory. Thus, it is applied to the small area of hardware implementation, which leads to faster computation in real time (Eisenbarth and Kumar 2007). The nodes in 6LoWPAN utilize the ECC algorithm, which can be applied to constrained devices.

Tables 2 and 3 provide summaries of the lightweight symmetric and asymmetric algorithms for the IoT environment based on their code length, block size, number of

Table 2 Symmetric lightweight cryptography algorithms for IoT

Symmetric algorithm	Code length	Structure	Number of rounds	Key size	Block size	Possible attacks
AES	2606	SPN	10	128	128	Man-in-middle attack
HEIGHT	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related key attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not fixed	ARX	20	16	32	Differential attack

Table 3 Asymmetric lightweight cryptography algorithms for IoT

Asymmetric algorithm	Key size	Code length	Possible attack
RSA	1024	900	Modules attack
ECC	160	8838	Timing attack

rounds uses in the algorithms, key size, internal structures, and possible attacks.

3.3.3 Lightweight encryption schemes in cloud computing

In this subsection, we discuss research that has been carried out on lightweight encryption schemes in cloud computing, which is also shown in Table 4.

Huang et al. proposed secure and efficient data collaboration with Attribute-Based Encryption (ABE) in cloud computing (Huang et al. 2016). They described the fine-grain access control of cipher text and they explained how data is secured in ABE (Naruse et al. 2015). In this collaboration scheme, the authorized user can decrypt the cipher text and perform write operation among them.

A Proxy Re-Encryption (PRE) for cloud data sharing has been suggested by Liang et al. It gives viability to information sharing as the information proprietor nevertheless utilizing resource constrained devices, such as cell phones and sensor nodes, can offload the majority of the computational operations to the cloud. Since its introduction, numerous variations of PRE have been proposed. They used Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABE) notation for PRE (Liang et al. 2015).

Fugkeaw et al. proposed a Very Lightweight PRE (VL-PRE) (Fugkeaw and Sato 2016).Their scheme provides flexible and scalable mobile revocation management in the cloud system. VL-PRE includes a three phase key generation, re-encryption key update, and re-encryption key renewal, which support resource-constrained mobile devices. Liang et al. developed a hybrid encryption algorithm for lightweight data stored in a cloud. Their algorithm solved the security issues and challenges of cloud data storage (Liang et al. 2016). This hybrid algorithm improves the RSA algorithm by increasing the key to generate large prime numbers and then combines it with the AES algorithm. They also described their experimental results where the hybrid algorithm has fast encryption and decryption, is more secure, and can easily resolve issues connected to lightweight data.

Baharon et al.'s research (Baharon et al. 2015) suggested a new lightweight encryption scheme for mobile cloud computing. They introduced the Lightweight Homomorphic Encryption (LHE) scheme, which reduces computation power during key generation and the encryption process.

Zegers et al. described a lightweight encryption and security handshaking protocol for the smartphone cloud. They aimed to solve the issues related to the limited resources of smartphones and the lack of awareness by users about security. They developed an encryption algorithm that secures the data before it is transferred to the cloud storage and that consumes less power (Zegers et al. 2015).

3.3.4 Lightweight encryption schemes for IoT

In this subsection, we discuss some of the existing research on lightweight encryption schemes for IoT, which is also shown in Table 5.

Yao et al.'s research (Yao et al. 2015) presented a lightweight no-pairing attribute-based encryption for ECC that they proposed in order to counter the security issues and challenges in IoT. They considered the issues of resource-constrained devices in IoT networks. Therefore, they utilized the Elliptic Curve Decisional Diffie Hellman (ECDDH) problem instead of the bilinear Diffie Hellman assumption. Their proposed scheme helps to improve execution efficiency and reduce communication costs.

Yang et al. proposed a novel dispersed secure information administration using keyword retrieval system for wellbeing IoT (Yang et al. 2016). Since patients are typically overseen by a variety of medical institutions the proposed system allows for the distributed access control of Protected Health Information (PHI) between different healthcare providers. Alternately, the aggregation of Electronic Health Records (EHRs) makes viable information recovery a test undertaking. The proposed scheme provides

Table 4 Summary of existing scheme on lightweight encryption scheme in cloud computing

References	Existing scheme	Basic theory	Description	Other feature
Huang et al. (2016)	Secure and efficient data collaboration in cloud computing	Attribute-based signature hierarchical—ABE, CP, bilinear map	Data collaboration scheme is presented in which authorized user can encrypt and decrypt data as well as perform write operation	Efficiency, compute complexity, correctness, data confidentiality, un forge ability
Liang et al. (2015)	Efficient ciphertext policy for cloud data sharing	PRE, CP-ABPRE, ABE	Define IND-CCA security notation for CP-ABPRE system	Efficiency improvement, security analysis, network profile secure
Fugkeaw and Sato (2016)	Improved lightweight PRE in cloud computing	PRE, VL-PRE, Collaborative- Ciphertext Policy-Attribute Role based Encryption (C-CP-ARBE), bilinear map	It exploits the reduction of size of root decryption key and relies on key update rather key generation	Key-updating, security analysis, flexibility, scalability
Liang et al. (2016)	Hybrid encryption of lightweight data in cloud storage	AES, RSA, DES, Miller–Rabin prime number detection algorithm	Improvement RSA algorithm for generating big prime numbers using three stages: search, pre-treatment, and detection	Security, feasibility, efficiency
Baharon et al. (2015)	Lightweight encryption scheme for mobile cloud computing	LEH, homomorphic encryption	Focused on the evaluation of total execution of LHE and compared scheme	Efficiency, minimize computation power, data encryption and evaluation, transmission time
Zegers et al. (2015)	Lightweight encryption and security protocol for smartphone cloud	CBC mode, key derivation, column permutation, row rotation, PBKDF2	Lightweight encryption algorithm designed on mobile devices	Reduce power consumption, encrypt large data volume, data security

Table 5 Summary of existing scheme on lightweight encryption scheme for IoT

Reference	Existing scheme	Basic theory	Description	Other feature
Yao et al. (2015)	Lightweight ABE based encryption for IoT	ABE, ECC, Diffie–Hellman, ECDDHP	The proposed lightweight ABE method is the KP-ABE method, and involves a central attribute authority and users	Key generation attributes, security, overhead analysis, efficiency
Yang et al. (2016)	Lightweight secure data for health IoT	PHI, HER, DBDH, LDAC-KS system	The proposed system enables distributed access control of protected health information among different medical domains	Overhead reduction, security analysis, reduce computation time
Sahraoui and Bilami (2015)	Lightweight end-to-end security in IoT	DTLS, HIP-DEX, HIP-BEX, CD-HIP, 6BR, DH	Paper present 6LoWPAN compression model and distribution scheme for HIP base exchange	Optimal efficiency, reduce energy consumption, protect against DoS attack
Al Salami et al. (2016)	Lightweight encryption for smart home	Identity-Based Encryption, private key generator, PKI	LES to be used for smart home applications and scheme have two-sub algorithms, called “KEYEncrypt” and “DATAEncrypt”	Flexible public key management, efficiency, reduce cost
Baskar et al. (2016)	Lightweight cryptography for resource constraint environment	ALTERA DE1, Blowfish, XTEA algorithm, chaotic map theory	A lightweight cryptographic algorithm by minimum calculation using a chaos map based key has been proposed and implemented in a FPGA	Strong security, increase performance
ERNEST (2017)	Lightweight cryptography for the IoE	SPONGENT hash function	New technology and lightweight primitives for the next generation of lightweight cryptography is suggested	IoE primitives’ drivers: binary code size, memory metrics and execution time

an efficient keyword search function on cross-domain PHI. Designing a lightweight algorithm with a secure data management system is essential for devices with limited health resources.

Sahraoui et al.'s research (Sahraoui and Bilami 2015) addressed the fact that WSN is a vital component of IoT. WSNs allow the representation of IoT, which makes it possible to express the real world dynamic characteristics in the virtual world of the Internet. WSNs require resource-constrained devices as well as possibly linked to communication security and end user privacy protection. They suggested a 6LoWPAN compression for the header of a Host Identity Protocol (HIP) packet.

Lightweight encryption for the smart home was addressed by Al Salami et al. Smart homes are one of the popular applications of IoT. It is a place in which a variety of resource-constrained devices communicate over the integrated network. They discussed the security and privacy issues of devices in a smart home, and they suggested a lightweight encryption algorithm for this setting. Their scheme provides the advantages of confidentiality without overhead cost, adoptability, and favorable level of efficiency (Al Salami et al. 2016).

Baskar et al.'s research (Baskar et al. 2016) described WSN as being the integration of a number of small, low power autonomous devices. By very natural, WSN tends to attack, even with the most familiar networks it is difficult to manage safely administrator.

Therefore, a lightweight cryptographic algorithm by minimum calculation that uses a chaos map-based key has been proposed and implemented in a Field Programmable Gate Array (FPGA). Its performance is analysis of the proposed algorithm that analyzed by encrypting sensor data and compared with other lightweight algorithms in the literature. Perform power FPGA, 1550 logic gates with 128 bit of key size are used and maximum through put of 200 kbps is achieved.

Lightweight cryptography for Internet of Everything (IoE) has been addressed by Ernest (Ernest 2017). He discussed the new technology and lightweight primitives for the next generation of lightweight cryptography. A lightweight cipher for an IoE device considers its size, speed, and simplicity. In addition, it also takes into account that the three primary drivers of IoE are binary code size, memory metrics, and execution time.

4 Proposed hybrid lightweight algorithm: HLA

4.1 HLA

In this section, we suggest a Hybrid Lightweight Algorithm (HLA), which is the combination of lightweight symmetry and lightweight asymmetric encryption algorithms for IoT devices.

Based on existing research many researchers have already developed lightweight cryptographic algorithms. Lightweight symmetric and asymmetric algorithms provide confidentiality, integrity with small key size and less computation power as well as require less memory space.

Lightweight asymmetric algorithms do have bigger key size, more computation complexity in the constrained IoT (Kar and Mishra 2016; Maity and Park 2016) environment, but provide stronger security than symmetric algorithms. Therefore, by considering all the aspects of lightweight symmetric and asymmetric algorithms it is necessary to develop an algorithms that bring all the features of symmetry and asymmetry lightweight algorithms in such a way that it minimize computation time, consume less power, is fast efficient and assures all the possible security.

In this section, we propose an idea that helps to implement it in a constrained IoT environment and provide security. We also provide the application service scenario of a smart home.

Smart spaces exist in the IoT compatible computing environment and create an application infrastructure for building and providing value added services that are based on the cooperative activities of human or machine environmental participants. The smart space paradigm seeks to build an advanced service infrastructure that allows computing vision like smart object is being executed on digital devices. A smart space has many components, such as a smart city, smart home, smart factory, and smart hospital, as shown in Fig. 2. These smart space components consist of a variety of resource-constrained devices that are interconnected and that communicate over a network. For example, as shown in Fig. 2, the devices used for smart toll collections, smart street light, street cameras, smart city data centers, and help to create a smart city. Similarly, other components like smart home have smart devices like smart light, smart heater, smart door and smart socket that are interconnected and communicated over the network. All of these are resource-constrained devices that require a lightweight encryption scheme. Some of the devices store sensitive information. For example, a door lock system stores the lock code number and some devices only store raw data. Also, in the medical system and smart factory many small low constrained machines like ECG machine, smart monitors, smart CT scan machine, smart alarm, smart PLC, smart vacuum pressure and many more are included in smart space. In addition, many devices have limited memory space, computational power, and battery power, but some of them have enough memory, processing power, and battery power.

Therefore, by considering all the parameters of these devices, we are proposing a scheme that combines the

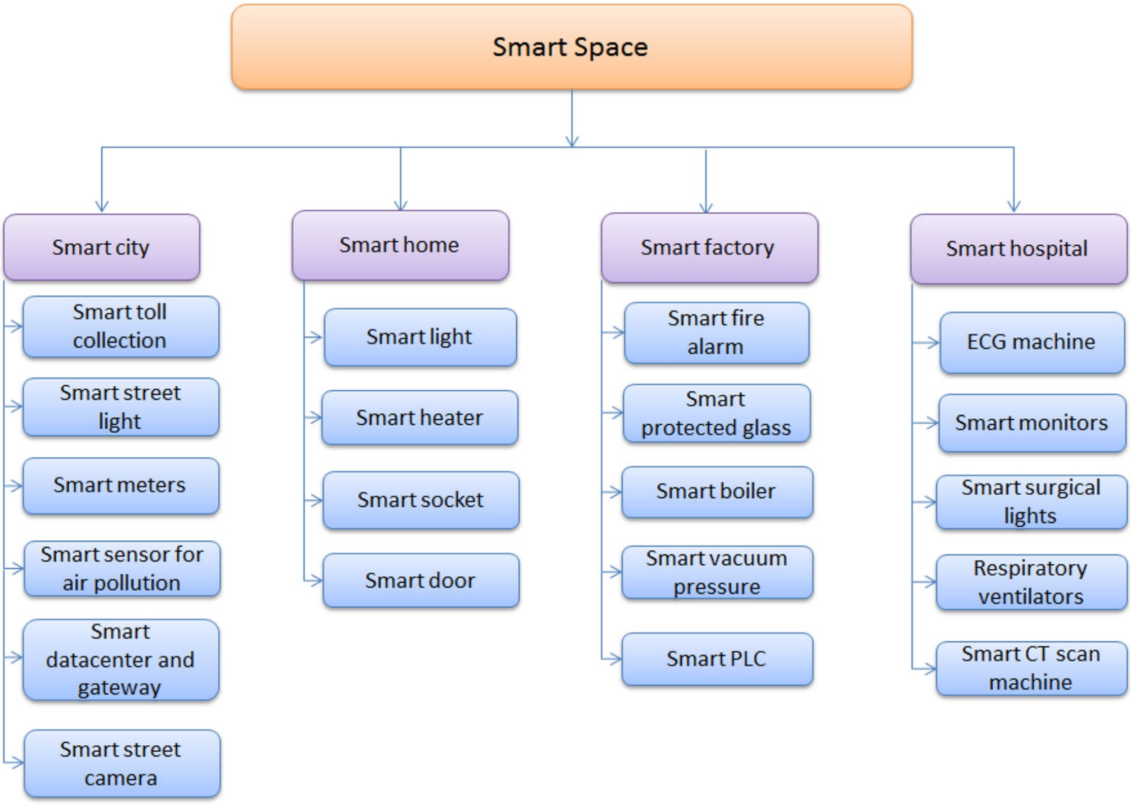

Fig. 2 Smart space components and devices

lightweight symmetric and asymmetric encryption algorithms for a specific IoT device, as shown in Fig. 3.

Figure 3 contains a flowchart in which the input is an IoT device and the output proposes the suitable encryption scheme for that device. This approach uses the following four parameters of a particular device as inputs: data size, memory space, computation power, and battery power. The threshold value of each parameter can be calculated by a specific algorithm.

The threshold value of memory space can be considered with memory technologies that combine a RAM drive's read and write speeds with the non-volatility of flash, which can be used to design fast and reliable file systems. In a nonvolatile semiconductor memory device, the first dynamic reference cell and the second dynamic reference cell perform the same rewriting operation as the memory cell. Since the data in the flash memory is rewritten several times, there is a decrease in writing speed. Due to this, the threshold value of the memory cell of the core circuit tends to decrease. On the other hand, since the data in the reference cell is not usually rewritten, the threshold value of the reference cell remains fixed. Consequently, as the number of times of rewriting increases, a sufficient read margin cannot be ensured due to the fixed threshold value of the reference cell. In the case of the selection of computational power threshold, one can consider the Boolean functions which can be composed of and, or not, gates in the circuit, which are threshold functions. In addition, in the Near-Threshold Computing (NTC) method, electronic devices operate at lower than normal voltages, which reduces energy consumption. Researchers predict that NTC could allow future computer systems to reduce energy requirements by 10–100 times or more by optimizing them for low-voltage operation. Reducing energy consumption is essential for enabling the continuation of Moore's law, which states that the number of transistors in a chip doubles around every 2 years. The battery capacity is measured in milliamp-hours, which are a measure of how many hours a battery can sustain a constant draw of current. When a device requires a wireless connection, choosing which protocol to use is an important factor that affects battery life.

The proposed HLA is based on levels of hierarchy. Smart home automation devices can include processors that receive, execute, and create the data objects for a particular device that confirms the hierarchal structured model (Hood et al. 2010). The HLA scheme provides two encryption schemes based on the analysis of device parameters. These two encryption schemes are lightweight symmetric and lightweight asymmetric encryption algorithms. These two algorithms are the improved version of conventional

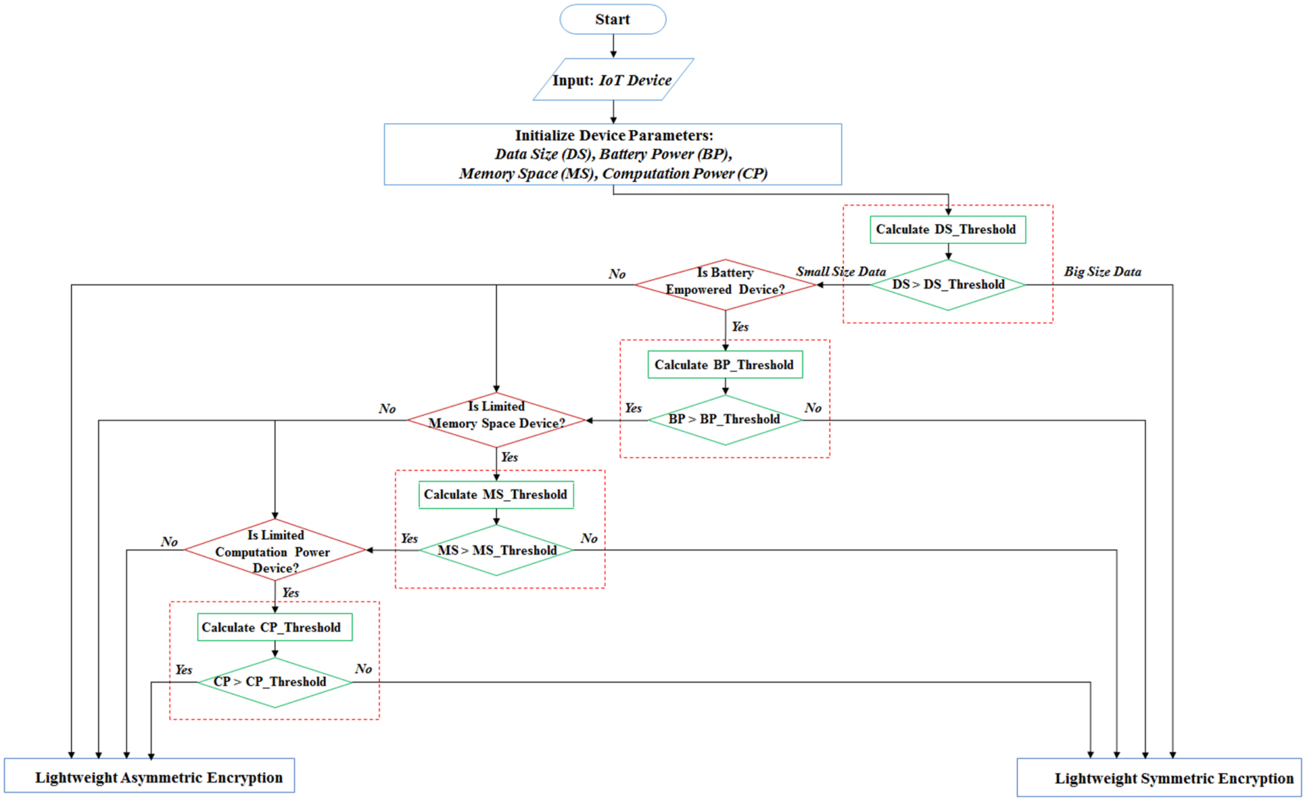
Start
Input: IoT Device
Initialize Device Parameters:
Data Size (DS), Battery Power (BP),
Memory Space (MS), Computation Power (CP)
Calculate DS_Threshold
DS > DS_Threshold
Small Size Data
Big Size Data
Is Battery Empowered Device?
No
Yes
Calculate BP_Threshold
BP > BP_Threshold
Yes
No
Is Limited Memory Space Device?
No
Yes
Calculate MS_Threshold
MS > MS_Threshold
Yes
No
Is Limited Computation Power Device?
No
Yes
Calculate CP_Threshold
CP > CP_Threshold
Yes
No
Lightweight Asymmetric Encryption
Lightweight Symmetric Encryption

Fig. 3 Proposed HLA

algorithms as they reduce the code length, number of rounds, key size, and block size. The lightweight symmetric and asymmetric algorithms are focused on low-constrained devices. The applications of HLA scheme include the Wireless Sensor Network (WSN), Radio-frequency Identification (RFID), IoT, and many more. Therefore, our proposed HLA scheme is very suitable for these low-constrained device environments. The HLA scheme is also comprised of four analysis phases, which are described below.

- *Data size (DS)* This is the first phase of the proposed scheme. First, HLA analyzes the size of data that is being transmitted over the network. Since all data is in electronic form and a lot of it is conveyed through computer applications, the size of the data is the first parameter to consider, and then, the information must be secured through different cryptographic algorithms.
- *Battery power (BP)* After the amount of data to transmit throughout the network has been analyzed, a smart device's battery power is another important factor. As we know, the power components of any source of power being provided to the device. There are much way to provide the power such as main power supply, battery, solar system, and many more. For the smart devices it may be smart battery. The battery power parameter requires input about a device's energy consumption.
- *Memory space (MS)* This is the third phase of the HLA scheme because how much memory is required for the computation of the data. The reason this is such an important component for smart devices is that the requirement of memory will increase with the complexity of the operations being performed by a smart device (Zegers et al. 2015). Therefore, based on memory size, the HLA scheme can determine which cryptographic encryption scheme should be applied.
- *Computation power (CP)* This is the final analysis phase of the HLA scheme. The need for an adequate processing component is evident. As intelligence in devices increases, so do the requirement for their operations to be able to execute the data faster and more efficiently (Davy 2003). Based on memory space, a device's battery power, and data size, a device's computation power is taken into considered. In a cryptosystem, the lightweight asymmetric encryption scheme generally requires more operation results as it needs more computation power than the lightweight symmetric encryption scheme.

After these four parameters have been initialized, HLA scheme first takes into account the amount of data to be transmitted over the network. If the size of the data is greater than the threshold value, it is considered to be large data, and based on the existing research (Masram et al. 2014a; Mushtaque 2014; Ahamad and Abdullah 2016) recommended for lightweight symmetric encryption, otherwise it goes for the subsequent analysis phase. During the next analysis phase, the battery parameter of the IoT device is considered. Some of the IoT devices are battery powered and some are not. The Eqs. (1), (2), and (3) can also affect the battery power, memory space, and computational power of the device respectively (Mohd et al. 2015b).

As for as battery is concerned, Stéphane Badel et al. noted the weakness of the efficiency metric and the dependency of power consumption on technology and the simulation method (Badel et al. 2010). To address these issues, they proposed a figure-of-merit (FoM), which includes the influence of power, and it is process-independent. FoM is expressed as:

$$\mathrm{FoM} = \frac{\mathrm{Th}}{\mathrm{GE}^2} \tag{1}$$

Two designs with the same GE may have different dynamic power due to different switching activities. Furthermore, standard- cell libraries include slow low-leakage cells and fast leaky cells that have the same footprints. The notations are explained in Table 6.

If the battery power of the device is less than the threshold value, then based on the previous research (Kim et al. 2016; Xiao et al. 2016; Karuppiah et al. 2015), the proposed method recommended to lightweight symmetric encryption. In addition, if the device has sufficient battery power the device will go for memory space analysis. Regarding the memory size, some of the metrics are platform dependent, such as the code size, which depends on the instruction set of the targeted processor. Memory size can also be affected by the addition XOR and the number of shifts. If the cipher text does not use substitution boxes, it does not require much memory. The design throughput expressed as:

$$\mathrm{Th} = \frac{\mathrm{N_B}}{\mathrm{T_B}} = \frac{\mathrm{N_B} \times \mathrm{F}}{\mathrm{C_B}} \tag{2}$$

Throughput is a function of design frequency. The number of cycles depends on the processor instruction set, which is stored in the memory. Thus, the frequency and number of cycles vary from one processor to another. Comparing software throughput across platforms is not very accurate. Synthetic metrics are used to combine two or more non-correlating metrics to capture various aspects of the performance. An example of synthetic metrics is “Code_Size×Cycle_Count/Block_Size”. Some IoT devices have limited memory and some have enough memory space to store the data. The HLA scheme checks whether the device has limited memory is recommended for computation power analysis, otherwise the lightweight asymmetric encryption is applied to the device data (Chandra et al. 2014; Nguyen et al. 2015; Verma et al. 2015).

In the last analysis phase of HLA, the computational power of the device is considered as the performance efficiency, which is defined as the ratio of the throughput calculated at a fixed clock frequency over the area (Kerckhof et al. 2012; Rolfes et al. 2008). It measures the cost of area and required to process a single cipher text bit, and is expressed as:

$$\mathrm{Efficiency} = \frac{\mathrm{Th}}{\mathrm{A}} = \frac{\mathrm{N_B}}{\mathrm{T_B} \times \mathrm{A}} = \frac{\mathrm{N_B} \times \mathrm{F}}{\mathrm{C_B} \times \mathrm{A}} \tag{3}$$

HLA also checks the computational power of the device and compares it with the threshold value by taking a device’s efficiency levels into account and then based on the existing research (Masram et al. 2014b; Puthal et al. 2017; Tripathi and Agrawal 2014), if the value computation power is less than threshold value, the device is recommended for lightweight symmetric encryption else lightweight asymmetric encryption.

Table 6 Metric notations

Notation	Metric
GE	Gate equivalent
NB	Block size
TB	Time to encrypt one block
CB	Number of cycles to encrypt one block
A	Design area
Th	Throughput
F	Frequency

4.2 Service scenario

We designed our proposed scheme for low-resource constrained devices with limited battery life and memory storage. This scheme can be applied in a smart home environment. Our proposed scheme has been designed for low-constrained devices that have limited resources, battery power, and memory space. Among the different types of smart space, the proposed HLA scheme is suitable for the smart home application. In a smart home, various IoT devices with different memory spaces, processing power, and battery capacities are interconnected and communicate with each other. The HLA scheme can be applied to a smart home application, as shown in Fig. 4.

Figure 4 shows the scenario of smart sensor node in smart home network, which communicate their lightweight encrypted secret message by using the HLA scheme.

The suggested scenario is smart sensor node in smart home network as described below.

Smart sensor node in a smart home network This scenario considers smart sensors for communications as shown in Fig. 4. In this scenario, the smart sensor sends very light message in the smart home network. Therefore, this is the case of small size data in the HLA scheme. These sensors have limited battery, memory, and computation power. Table 7 shows the sensor node parameter values. In this table, we calculated the threshold value which is the average of battery power, memory space, and computation power respectively.

For example, a smart sensor device can sense the data from the smart home environment. Suppose one smart sensor node wants to send the data to another sensing device, then for secure and efficient communication, we considered following parameters as shown in Table 7 in HLA scheme. The threshold value of battery power is 11.66 mW, if the sensor node has the battery power 10 mW (data 2) which is less than the threshold value which results to the lightweight symmetric encryption. If we consider the data 3 of battery power which is greater than threshold value, it goes to next phase analysis which is memory space.

Table 7 Smart sensor node parameters value (Kerckhof et al. 2012)

Parameter	Data (1)	Data (2)	Data (3)	Threshold value (average)
Battery power (mW)	13	10	12	11.66
Memory space by considering throughput (byte)	4740	2195	2997	3310.66
Computation power by considering frequency (MHz)	444	377	363	399

In the memory, phase analysis considers the throughput to evaluate the threshold value. As shown in Table 7, the average threshold value of the memory spaces of different IoT devices is 3310.66 bytes and if sensor node has the memory space 4740 bytes (data 1), which is greater than the threshold value. As a result, the device goes to the computation analysis phase, otherwise it refers to lightweight symmetric encryption. Commutation power considers the frequency of the processor of smart sensor. As shown in Table 7, the threshold value of a computation parameter is 399 MHz and if we consider data 2 (377 MHz) and data 3

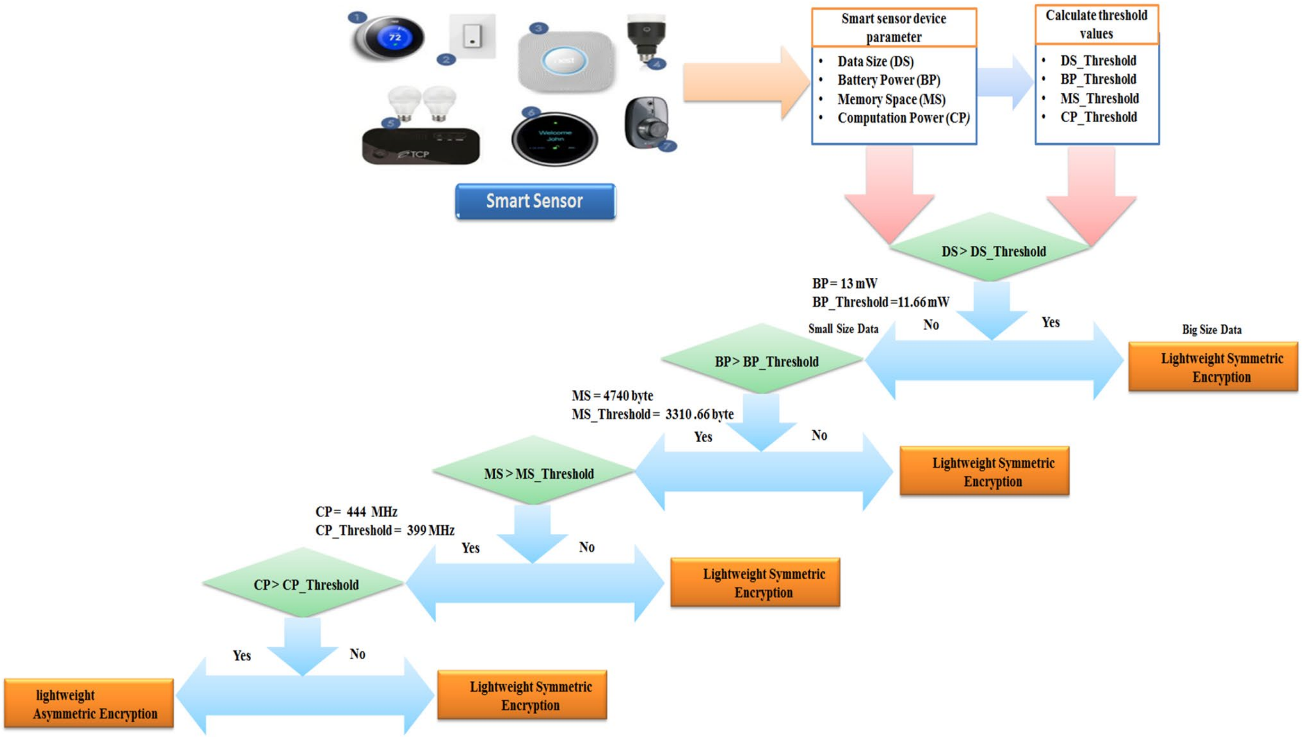

Fig. 4 Service scenario of smart sensor node in smart home

(363 MHz) the HLA scheme results the lightweight symmetric encryption and if we consider data 1 (444 MHz) it goes to lightweight asymmetric encryption.

4.3 Open issues and discussions

Contributions in cryptographic design and implementation are important, but there are still areas to be considered in future research works. In the previous chapters of this paper, we surveyed many existing lightweight encryption schemes for constrained IoT devices. In addition, we summarized various lightweight cryptographic encryptions techniques on big data, mobile cloud computing, and distributed computing. In this section, we aim to emphasize research topics related to conventional and lightweight cryptographies. The issues to be addressed are as described below.

- *Cipher structure and implementations* The cryptographic implementation investigated in this paper helps to show the overall performance of various cryptographic designs. However, a reliance on tools and technologies distinctly distorts the results, resulting in large deviations between the studies. Therefore, it is important to think of another solution and to depart from the general paradigm propose another cryptosystem to compare with existing ones. This new paradigm could help to improve the quality of research in the field of lightweight cryptography. For optimizing cryptographic energy, Mohd et al. proposed a hardware impact design energy that achieved the optimum energy for Katan cipher implementing in 32 rounds (Mohd et al. 2015b). Moreover, they suggested building a more compact model that takes algorithmic, architectural and physical problems into account. It includes a cipher structure like slow diffusion of traditional Feistel structure. In addition, balancing between number of rounds increased and round complexity, pipelining, rolling and unrolling rounds. Moreover, Negash et al. suggested a lightweight data interchange for IoT in a PalCom middleware framework (Negash et al. 2016).
- *Issues related with block size and key size* The size of key and block length plays an important role in the development of lightweight cryptography for resource-constrained devices. If the key size is increased then the cipher text size is also increased, which requires higher computational power. This is also applicable to block length. A multi-key attack is one of the major issues in which the attackers break the encryption under one particular key. The confidentiality property can be compromised if the attackers successfully get the key.
- *New attacks* There are several countermeasures that can be implemented to prevent security attacks. Nevertheless, as with countermeasures to prevent known attacks, new attacks can overwhelm the implemented measures (Bhunia et al. 2013). Therefore, the cipher's ability to resist attacks should be updated. In a resource-constrained environment, the Hardware Trojan (HT) is a big issue. HT is a malicious change in the embedded circuit either during the design or fabrication stage, and it is completely characterized by its physical appearance and behavior. Another unresolved issue is the need to develop a widespread model that incorporates hardware and HT design to analyze security trade-offs and complexities.
- *Security metrics* A constrained device security level is as flexible as its system resources (Hayajneh et al. 2014). This enhances the importance of security metrics. Paradoxically, there is no security metric that can accurately measure or estimate cryptographic security. Currently, encryption is subject to decryption that is aimed at breaking the encryption algorithm by using a series of attacks. Based on these reported successful attacks, the level of encryption is designated as being safe less secure, moderate, or unsafe. Nevertheless, current security systems are still in need of improvements but analyzing cryptographic security remains a challenging issue. As such, we still require more clearly-defined security standards for analyzing cryptographic security for constrained devices in IoT environment.

5 Conclusion and future directions

In this paper, we have gone over lightweight cryptographic algorithms in detail. Many low-resource devices perform computations in an IoT environment. These devices are limited in regards to memory, battery life, power consumption, and computations. IoT devices also face the challenges of security and privacy as well as the issue of how to maintain trust between IoT users. Furthermore, we summarized different kinds of lightweight cryptographic algorithms that are easy to use for hardware and software implementations. Some cryptographic algorithms are vulnerable to some kinds of attacks, which we also described in the paper. It is important to develop more secure and lightweight encryption algorithms that have a smaller key size, fast processing, and require less computation power. In this paper, we proposed a scheme that can be applied in the smart home environment. We also discussed open issues in terms of cipher structure, implementation, block size, key size, new attacks, and security metrics.

In the future, we will examine how expensive these solutions are and if it is possible to implement them in a constrained environment. In addition, an algorithm for calculating the threshold value of each device parameter, which has already been laid out in our proposed scheme, should be developed.

Acknowledgements This work was supported by Institute for Information and communications Technology Promotion (IITP) grant funded by the Korea government (MISP) (No. B0190-16-2030, Web Service User Account Information Management and Spill/Exploit Detection Technology Development).

References

Ahamad MM, Abdullah MI (2016) Comparison of encryption algorithms for multimedia. Rajshahi Univ J Sci Eng 44:131–139

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

Aumasson JP, Henzen L, Meier W, Naya-Plasencia M (2013) Quark: a lightweight hash. J Crypto 26(2):313–339

Babbage S, Dodd M (2008) The MICKEY stream ciphers. In: Proceeding of New Stream Cipher Designs, Springer, Berlin, pp 191–209

Badel S, Dağtekin N, Nakahara JJ, Ouafi K, Reffé N, Sepehrdad P, Vaudenay S (2010) ARMADILLO: a multi-purpose cryptographic primitive dedicated to hardware. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin. pp 398–412

Baharon MR, Shi Q, Llewellyn-Jones D (2015) A new lightweight homomorphic encryption scheme for mobile cloud computing. In: Proceeding of 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), IEEE. pp 618–625

Bansod G, Raval N, Pisharoty N (2015) Implementation of a new lightweight encryption design for embedded security. IEEE Trans Inf Forens Sec 10(1):142–151

Bansod G, Patil A, Sutar S, Pisharoty N (2016) An ultra lightweight encryption design for security in pervasive computing. In: Proceeding of 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, pp 79–84

Baskar C, Balasubramaniyan C, Manivannan D (2016) Establishment of light weight cryptography for resource constraint environment using FPGA. Proced Comput Sci 78: 165–171

Beaulieu R, Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L (2015) The SIMON and SPECK lightweight block ciphers. In: Proceeding of 52nd ACM/EDAC/IEEE, Design Automation Conference (DAC), IEEE, pp 1–6

Bhunia S, Abramovici M, Agrawal D, Bradley P, Hsiao, MS, Plusquellic J, Tehranipoor M (2013) Protection against hardware trojan attacks: towards a comprehensive solution. IEEE Des Test 30(3):6–17

Biswas K, Muthukkumarasamy V, Singh K (2015) An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sens J 15(5): 2801–2809

Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Vikkelsoe C (2007) PRESENT: an ultra-lightweight block cipher. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, pp 450–466

Bogdanov A, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y (2008) Hash functions and RFID tags: mind the gap. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, pp 283–299

Bogdanov A, Knežević M, Leander G, Toz D, Varıcı K, Verbauwhede I (2011) SPONGENT: a lightweight hash function. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, pp 312–325

Bossuet L, Grand M, Gaspar L, Fischer V, Gogniat G (2013) Architectures of flexible symmetric key crypto engines—a survey: from hardware coprocessor to multi-crypto-processor system on chip. ACM Comput Sur 45(4):1–41

Buja AG, Latip SFA (2015) The direction of lightweight ciphers in mobile big data computing. Proced Comput Sci 72:469–476

Chandra S, Paira S, Alam SS, Sanyal G (2014) A comparative survey of symmetric and asymmetric key cryptography. In: Proceeding of 2014 International Conference on Electronics Communication and Computational Engineering (ICECCE), IEEE, pp 83–93

Davy A (2003) Components of a smart device and smart device interactions, Telecommunications Software and Systems Group, pp 1–18

ECRYPT (2017) eSTREAM: the ECRYPT stream cipher project. http://www.ecrypt.eu.org/stream/. Accessed 16 Jan 2017

Eisenbarth T, Kumar S (2007) A survey of lightweight-cryptography implementations. IEEE Desi Test Comput 24(6):1–12

Ernest W (2017) Light primitives and new technologies are driving the next generation of lightweight cryptography. http://semiengineering.com/lightweight-cryptography-for-the-ioe/, Accessed Feb 2017

Fan X, Mandal K, Gong G (2013) Wg-8: a lightweight stream cipher for resource-constrained smart devices. In: Proceeding of International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Springer, Berlin, pp 617–632

Feldhofer M, Rechberger C (2006) A case against currently used hash functions in RFID protocols. In: Proceeding of OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Springer, Berlin, pp 372–381

Fugkeaw S, Sato H (2016) Improved lightweight proxy re encryption for flexible and scalable mobile revocation management in cloud computing. In: Proceeding of 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), IEEE, pp 894–899

Grand M, Bossuet L, Le Gal B, Gogniat G, Dallet D (2011) Design and implementation of a multi-core crypto-processor for software defined radios. In: Proceeding of International Symposium on Applied Reconfigurable Computing, Springer, Berlin, pp 29–40

Guo J, Peyrin T, Poschmann A (2011) The PHOTON family of lightweight hash functions. In: Proceeding of Annual Cryptology Conference, Springer, Berlin, pp 222–239

Guo P, Wang J, Ji S, Geng XH, Xiong NN (2015) A lightweight encryption scheme combined with trust management for privacy-preserving in body sensor networks. J Medi Sys 39(12):190–198

Hayajneh T, Doomun R, Al-Mashaqbeh G, Mohd, BJ (2014) An energy-efficient and security aware route selection protocol for wireless sensor networks. Sec Commun Net 7(11):2015–2038

Hell M, Johansson T, Meier W (2007) Grain: a stream cipher for constrained environments. Int J Wirel Mob Comput 2(1):86–93

Hirose S, Ideguchi K, Kuwakado H, Owada T, Preneel B, Yoshida H (2010) A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW. In: Proceeding of International Conference on Information Security and Cryptology, Springer, Berlin, pp 151–168

Hodjat A, Verbauwhede I (2004) High-throughput programmable crypto co-processor. IEEE Micro 24(3):34–45

Hood GW, Kappelhoff R, Hall KH (2010) US Patent No. 7,672,737. US Patent and Trademark Office, Washington, DC, pp 1–29

Hosseinzadeh J, Hosseinzadeh M (2016) A comprehensive survey on evaluation of lightweight symmetric ciphers: hardware and software implementation. Adv Comput Sci Int J 5(4):31–41

Huang Q, Yang Y, Shen M (2016) Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Fut Gen Comput Sys 72:239–249

Iokibe K, Maeshima K, Kagotani H, Nogami Y, Toyota, Y, Watanabe T (2014) Analysis on equivalent current source of AES-128 circuit for HD power model verification. In: Proceeding of 2014 International Symposium on Electromagnetic Compatibility, Tokyo (EMC'14/Tokyo), IEEE, pp 302–305

James M, Kumar DS. (2016) An implementation of modified lightweight advanced encryption standard in FPGA. Proc Technol 25:582–589

Kar J, Mishra MR (2016) Mitigating threats and security metrics in cloud computing. J Inf Process Sys 12(2):226–233

Karakoç F, Demirci H, Harmancı AE (2015) AKF: A key alternating Feistel scheme for lightweight cipher designs. Info Proc Lett 115(2):359–367

Karuppiah AB, Dalfiah J, Yuvashri K, Rajaram S (2015) An improvised hierarchical black hole detection algorithm in wireless sensor networks. In: Proceeding of 2015 International Conference on Innovation Information in Computing Technologies (ICIICT), IEEE, pp 1–7

Kerckhof S, Durvaux F, Hocquet C, Bol D, Standaert FX (2012) Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, pp 390–407

Kim JM, Lee HS, Yi J, Park M (2016) Power adaptive data encryption for energy-efficient and secure communication in solar-powered wireless sensor networks. J Sens 2016:1–10

Kitsos P, Sklavos N, Provelengios G, Skodras AN (2013) FPGA-based performance analysis of stream ciphers ZUC, Snow3g, Grain V1, Mickey V2, Trivium and E0. Microprocess Microsyst 37(2):235–245

Latré B, Braem B, Moerman I., Blondia C, Demeester P (2011) A survey on wireless body area networks. Wire Net 17(1):1–18

Leander G, Paar C, Poschmann A, Schramm K (2007) New lightweight DES variants. In: Proceeding of International Workshop on Fast Software Encryption, Springer, Berlin, pp 196–210

Lee JH, Lim DG (2014) Parallel architecture for high-speed block cipher, HIGHT. Int J Sec Appl 8(2):59–66

Li L, Liu B, Wang H. (2016) QTL: a new ultra-lightweight block cipher. Microproc Microsys 45: 45–55

Liang K, Au MH, Liu JK, Susilo W, Wong DS, Yang G, Yang A (2015) A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Fut Gen Comput Sys 52:95–108

Liang C, Ye N, Malekian R, Wang R (2016) The hybrid encryption algorithm of lightweight data in cloud storage. In: Proceeding of 2016 2nd International Symposium on Agent, Multi-Agent Systems, and Robotics (ISAMSR), IEEE, pp 160–166

Maity S, Park JH (2016) Powering IoT devices: a novel design and analysis technique. J Converg 7:1–18

Masram R, Shahare V, Abraham J, Moona R, Sinha P, Sunder G, Pophalkar S (2014a) Dynamic selection of symmetric key cryptographic algorithms for securing data based on various parameters. ArXiv preprint arXiv:1406.6221, pp 1–8

Masram R, Shahare V, Abraham J, Moona R (2014b) Analysis and comparison of symmetric key cryptographic algorithms based on various file features. Int J Netw Sec Appl 6(4):43–52

McKay KA, Bassham L, Turan M S, Mouha N (2016) Report on lightweight cryptography. NIST DRAFT NISTIR, pp 1–29

Mohd BJ, Hayajneh T, Vasilakos AV (2015a) A survey on lightweight block ciphers for low-resource devices: comparative study and open issues. J Netw Comput Appl 58:73–93

Mohd BJ, Hayajneh T, Khalaf ZA (2015b) Optimization and modeling of FPGA implementation of the Katan Cipher. In: Proceeding of 2015 6th International Conference on Information and Communication Systems (ICICS), IEEE, pp 68–72

Mushtaque MA (2014) Comparative analysis on different parameters of encryption algorithms for information security. JCSE Int J Comput Sci 2(4):76–82

Naruse T, Mohri M, Shiraishi Y (2015) Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. Human-centric Comput Inf Sci 5(1):8–25

Negash B, Rahmani AM, Westerlund T, Liljeberg P, Tenhunen H (2016) LISA 2.0: lightweight internet of things service bus architecture using node centric networking. J Ambient Intell Human Comput 7(3):305–319

Nguyen KT, Laurent M, Oualha N (2015) Survey on secure communication protocols for the internet of things. Ad Hoc Netw 32:17–31

Padmavathi B, Kumari SR (2013) A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution. Int J Sci Res 2(4):170–174

Peng C, Du X, Li K, Li M (2016) An ultra-lightweight encryption scheme in underwater acoustic networks. J Sens 2016:1–10

Puthal D, Nepal S, Ranjan R, Chen J (2017) A dynamic prime number based efficient security mechanism for big sensing data streams. J Comp Syst Sci 83(1):22–42

Rivest RL (1994) The RC5 encryption algorithm. In: Proceeding of International Workshop on Fast Software Encryption, Springer, Berlin, pp 86–96

Rolfes C, Poschmann A, Leander G, Paar C (2008) Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In: Proceeding International Conference on Smart Card Research and Advanced Applications. Springer, Berlin, pp 89–103

Sahraoui S, Bilami A (2015) Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. Comp Net 91:26–45

Sajid A, Abbas H, Saleem K (2016) Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges. IEEE Acc 4:1375–1384

Saputra H, Vijaykrishnan N, Kandemir M, Irwin MJ, Brooks R, Kim S, Zhang W (2003) Masking the energy behavior of DES encryption. In: Proceeding of the conference on Design, Automation and Test in Europe, vol 1 Computer Society, IEEE, pp 1–6

Shelby Z, Hartke K, Bormann C (2014) The constrained application protocol (CoAP), Internet Engineering Task Force (IETF), pp 1–110

Singh S, Jeong YS, Park JH (2016a) A survey on cloud computing security: issues, threats, and solutions. J Netw Comp Appl 75:200–222

Singh S, Sharma PK, Moon SY, Moon D, Park JH (2016b) A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. J Supercomp. doi:10.1007/s11227-016-1850-4

Singh S, Sharma PK, Park JH (2016c) Secure clouds forensic investigative architecture for social network cloud. Adv Sci Lett 22(9):2461–2464

Souissi R, Ben-Ammar M (2014) An intelligent wireless sensor network temperature acquisition system with an FPGA. Wire Sens Netw 6(1):1–7

STAMFORD (2013) Gartner says the internet of things installed base will grow to 26 billion units by 2020. http://www.gartner.com/newsroom/id/2636073. Accessed 16 Jan 2017

Standaert FX, Piret G, Rouvroy G, Quisquater JJ, Legat JD (2004) ICEBERG: an involutional cipher efficient for block encryption in reconfigurable hardware. In: Proceeding of International Workshop on Fast Software Encryption, Springer, Berlin, pp 279–298

Tillich S, Großschädl J (2006) Instruction set extensions for efficient AES implementation on 32-bit processors. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, pp 270–284

Tripathi R, Agrawal S (2014) Comparative study of symmetric and asymmetric cryptography techniques. Int J Adv Found Res Comp 1(6):68–76

Université du Luxembourg (2017) Lightweight block ciphers. https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers. Accessed 22 Jan 2017

Verma S, Pal SK, Muttoo SK (2014) A new tool for lightweight encryption on android. In: Proceeding of Advance Computing Conference (IACC), 2014 IEEE International, IEEE, pp 306–311

Verma D, Jain R, Shrivastava A (2015) Performance analysis of cryptographic algorithms RSA and ECC in wireless sensor networks. IUP J Telecommun 7(3): 51–65

Wheeler DJ, Needham RM (1994) TEA, a tiny encryption algorithm. In: Proceeding of International Workshop on Fast Software Encryption, Springer, Berlin, pp 363–366

Xiao C, Wang L, Zhu M, Wang W (2016) A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft. J Netw Comp Appl 59:117–125

Yang Y, Zheng X, Tang C. (2016) Lightweight distributed secure data management system for health internet of things. J Netw Comp Appl. doi:10.1016/j.jnca.2016.11.017

Yao X, Chen Z, Tian Y (2015) A lightweight attribute-based encryption scheme for the Internet of Things. Fut Gen Comp Sys 49:104–112

Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. Comput Netw 52(12):2292–2330

Yu J, Khan G, Yuan F (2011) Xtea encryption based novel RFID security protocol. In: Proceeding of 24th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, pp 58–62

Zegers W, Chang SY, Park Y, Gao J (2015) A lightweight encryption and secure protocol for smartphone cloud. In: Proceeding of 2015 IEEE Symposium on Service-Oriented System Engineering (SOSE), IEEE, pp 259–266

Zhou J, Cao Z, Dong X, Vasilakos, AV (2017) Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag 55(1):26–33