March-April 2020
ISSN: 0193-4120 Page No. 1293 - 1299

A Critical Review on LWC Algorithms for IOT Security

A. Mahesh Reddy[1], M. Kameswara Rao[2]
[1]Research scholar, [2]Associate Professor
Department of ECM, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, India.
[1]alumru.mahesh@gmail.com, [2]kamesh.manchiraju@gmail.com

Article Info
Volume 83
Page Number: 1293 - 1299
Publication Issue:
March - April 2020

Abstract

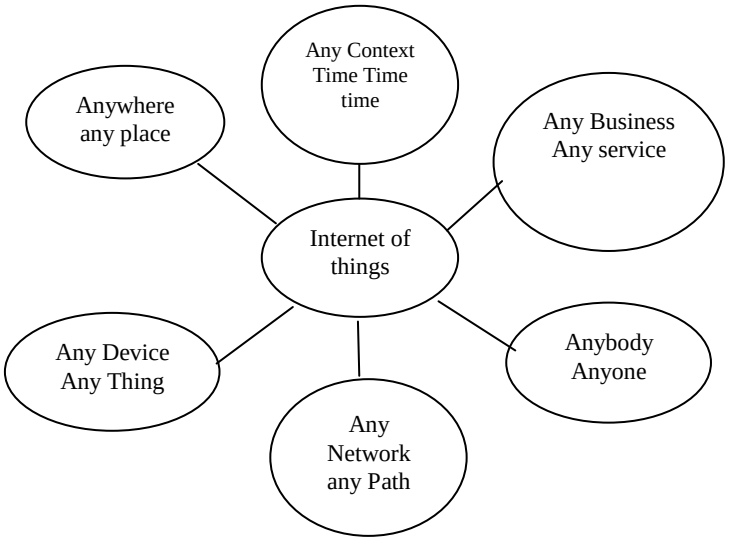
Internet of things (IOT) introduces capability to connect and identify different physical objects into unified system. IOT allows these objects to match computation and made network decisions. In such a disparate world computation, each one of IOT consumer will have a specific role to serve in the form of communication. There is a hazard that an unknown attacker can trash the protection of the network. A number of serious challenges are part of IOT about access to personal information related to the system and privacy of individuals. At this point protection and privacy becomes a major concern in the IOT. Security needs to establish; we need to be careful to maintain confidentiality, authentication, and non-repudiation as well as data integrity. From this article, we deal with different security issues in IOT, addressing different conventional IOT device security techniques and their flaws. Later we recognize a few appropriate algorithms for security; this survey summarizes the security threats.

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 14 March 2020*

***Keywords*:** CoAP, DoS, Data encryption, Internet of things (IOT), Lightweight algorithm, Privacy, RFID, Security.

1. Introduction

The Internet of Things enables electronic devices to participate actively in our environments through exchanging information with many other network users, making it possible to remember activities, adjustments in their environment and to behave and respond individually, mostly without any human cooperation [1]. IOT's benefits are nearly infinite and its implementation changes the way we live and work through consuming time, resources and creating new growth opportunities, creativity and sharing the information between entities. According to experts, IOT could grow dramatically by 2020 with more over 50 billion different detectable apps [2]. As shown in Fig. 1,



March-April 2020
ISSN: 0193-4120 Page No. 1293 - 1299

Figure 1: Definition of IOT

IOT's allow people and objects to be associated at any moment, anywhere for anything and everyone, preferably handling any path / network or service [3]. The overall intension was to build a "Better World for Humanity" through creating things close to us smart so that is how to recognize our needs to act appropriately without any people intervention. IOT has prominent stand in areas like sustainable ecosystems, smart grids, farming, industrial internet and wearables. IOT protection refers to data security, collected and transferred through IOT devices. It will be essential data transmitted via IOT devices be extremely protective, due to data transmitted between the systems is very private and significant, as it includes secret data, health situation and other private information. Hundreds of IOT-connected devices bear advance services to public around the world and lower costs [4]. Sadly, this will increase in the number of connected devices creates expanded security hazards, and risks are rapidly evolving. Several scholars around the globe are making use of their efforts to address different IOT security challenges. Nevertheless, IOT security is a major challenge owing to its heterogeneous design. Because the Internet of Things is a combination of so many devices, all of these systems have their own conventional security and privacy vulnerabilities that must be discussed in the IOT sense. Security should be examined because it preserves information against improper access and maintains confidentiality integrity and authenticity of the evidence. Confidentiality protects data can exposed to unauthorized persons, activities or processes. Intruders because of the protection of falsification or the manipulation of statistics define integrity. Authenticity relates to the checking of the identification of the unit. The security system can built-in to maintain data integrity, confidentiality, authentication and non-repudiation.

2. Research Motivation

IOT helps connect the dissimilar objects found in a heterogeneous world. Such style of transparency and much less human intervention will expose IOT to numerous attacks such as mid-attack person, Denial of service (DoS) attack. Furthermore, any system that contributes to unauthorized access will access the network. Such attacks can also physically destroy equipment and network connections. Essentially, this would deal IOT's security and privacy. As IOT is a resource restricted with much less power, latency, and not much storage, it requires a reliable security solution that is not chomping through IOT resources.

3. Security for IOT Devices

Intruders because of the protection of falsification or the manipulation of statistics define integrity. Authenticity relates to the checking of the identification of the unit [5] [6]. HTTP is an application layer framework for centralized, shared and hypermedia information systems and has been used for WWW data communication since 1990[7]. HTTP is considered as a stand-alone protocol and vulnerable as it sends data in encrypted form and does not use data protection security mechanisms. Increasing the transmission of sensitive data over the internet required a more secure method.

This has led to the establishment of Secure Socket Layer (SSL) under HTTP and then its Transport Layer Security (TLS) successor. This combo also known as HTTPS, a secure communication system cryptography performed to avoid from to eavesdropping, tampering, or messages [8]. HTTP and HTTPS operate the Transmission Control Protocol (TCP) transport layer protocol offering security, error prevention and data transmission flow control. Such features of data processing require additional support from systems to ensure efficient communication [9]. HTTP and HTTPS were not intended for resource-limited IOT devices and therefore an extremely powerful protocol was built exclusively for resource-limited devices. The constrained application protocol (CoAP) is a specific application layer protocol architecture for resource-restricted applications namely as IOT [10]. Alike HTTP, CoAP works using REST methods are developed and be able to communicate efficiently between the two protocols [10]. Unlike HTTP that usually runs via TCP, by default CoAP runs through UDP and this protocol needs fewer header information compare with TCP, can make more appropriate for limited devices. To design, UDP cannot search for bugs in the transmission of data and it is perceived to be an unstable protocol [10]. Because of the IOT's restricted nature, devices have limited resources and confined to what procedures and protocols they can substantiate. Although these type of devices can have minimal support, they might be capable of capturing and distributing sensitive personal information to network or cloud services across the internet. This raises problems when data shared on the internet is inherently vulnerable to attack and must be secured [11]. In an attempt to standardize restricted device connectivity associations like the IETF have established useful web standards for restricted devices like CoAP [10]. Security standards also developed because of the aim of protecting network-wide IOT sharing of data through modifying current TLS security protocols to restricted devices. A mechanism for protecting data exchange in some IOT systems, given by the corresponding DTLS protocol. DTLS preserves CoAP communications data security, integrity and reliability in a manner similar to that TLS covers web-based HTTP correspondence [12] [10] HTTPS. Although DTLS is ideal for few IOT devices, still it is a heavy weight protocol and therefore devices must have adequate resources to operate while still capable of performing the task calculated for the devices, such as collecting data from temperature sensors.

4. Secured IOT Architecture

IOT will ensure that all its layers are secure. Therefore,

March-April 2020
ISSN: 0193-4120 Page No. 1293 - 1299

IOT safety must not neglect the security of the whole devices that crosses the application layer, network layer, middleware layer, and physical layer.

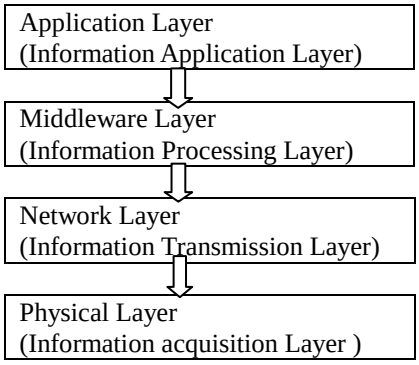


Figure 2: Secured IOT Architecture

4.1 Physical Layer

i) Physical Security Approach

This approach is supposed to be at the lowest and collect information over the IOT network. Many security issues occur during the collection of information and physical device safety. Sensors, sensor terminals and RFID codes may be the same as hardware.

a) Sensors Network Security Approach

This approach deals with several has drawbacks like physical capturing of sensor nodes, gateway nodes, attacks on privacy along with latency, DoS attack, eavesdropping attack, also attacks on node replication. Security approaches namely encryption protocols, key distribution protocols; intrusion detection protocols must be included in developing a safety architecture for the sensor network [13].

b) RFID Security Approach

RFID-related security problems include theft of RFID tag and device location information, sniffing attacks, man-in-middle attacks, duplication, reuse and modifying attacks. RFID authentication enforced in the most important cases through physical measures or computer systems, or sometimes both. Data encryption, blogger sign, jamming, destroy order policies are some of the physical security methods. LCAP, Hash Lock, Hash Set, re-encoding protocol [14] are few security protocols with RFIDs.

c) Sensors Terminals Security Approach

Illegal activity, misuse or harm to sensitive information, duplication SIM data, Air system knowledge imitation are main security problems connected to IOT sensor terminals.

ii) Information Acquisition Security Approach

In addition to safety issues of perception security, it is one task of the layer, understanding to address problems to security of data retrieval. Some of the possible attacks include security problems such as surveillance, manipulation hacking, and replay threats.

Security solution IEEE 802.15.4 is accessible on this layer but remains vulnerable to attacks.

4.2 Network Layer

a) Information transmission Security Approach

The primary task of the network layer, in the IOT system is to transfer data throughout the network, because IOT is built on primary communication platform; it is vulnerable to different intrusions like gateway intrusion, Denial of Service (DoS) attack, database intrusion and man-in-middle attack. Network layer protection policy will ensure reliability, privacy, transparency, and quality of data while data is sent over the network. To prevent these type of attacks, intrusion detection, authentication, key management, and negotiation could be added [15].

IPv6 with more addressing space. DES, AES can be applied using IPsec at network layer, using advanced cryptographic standards.

4.3 Middleware Layer

This layer duty to process the information and to provide access in the IOT layered framework through network layer and application layer. Some of the technical problems in middleware layer is linked to confidentiality, security and performance. Ensuring privacy and safe storage improves the security of the middleware layer.
Because UDP was an inaccurate method, a security method utilizing DTLS is included in this layer.

4.4 Application Layer

Privacy plays an important role for protecting information layer of the system. Security permissions must be limited, so that you can guarantee that the unauthorized person is entitled to control and use information. Information manipulation and data encryption technologies are the basic building blocks of information protection technologies, used to guarantee database safety [16]. Security, backup and recovery process need to be worked out well in order to manage a stable truth. Some of the protection methods for information include TLS, SSL, DNS, and many more. CoAP can be used for IOT devices constrained on this layer. Below Table gives summary of security protocol for every individual layer and their flaws.

Table 1: Security Protocols in IOT

Layer	Protocol Used	Security protocol	Attacks
Application	COAP	----------	----------
Middleware	UDP	DTLS	RC4, DoS
Network	IPV6, RPL	IPSec	DoS
Physical	IEEE 802.15.4, PHY,MAC	IEEE 802.15.4	Integrity, Authentication, DoS

4.5 Challenges in IOT

The key challenge of universal implementation is to integrate networks for Multi-Innovation standard all-IP system to ensure consistent quality and flexibility of communications systems. That is why; IOT is dependent on the availability and efficiency of current Network Technology Correspondence and IPv6 Convention that fulfills preconditions of tendency and versatility. The secondary threat is just to ensure security, privacy, privacy of data, and confidentiality of users. In fact, the process that handles authentication, permission, access control, and key management challenges significant and large IOT implementations. In addition, since the strengths of forced devices can communicate on the Internet are diminishing, it is necessary to improve security of edge systems for the global network.

A few other complexities are associated with the IOT process listed below:

- Some study on security vulnerabilities in IOT wireless sensor networks has already been examined, resulting in many attacks such as DoS / DDoS, response threats, eves dropping and many more.
- Another limitation is the use of resource-constrained systems in terms of power use, finite battery capacity, latency, different architectures, and complex protection measures that can slow system efficiency.
- More interference by humans may lead to physical and logical threats.

Thus, issues can be connected to things or to networks. Issues are about capacity limits, heterogeneous networks, and security and privacy. Issues related to the network include scalability, latency problems, security, and privacy.

4.6 Issues in IOT

IOT is widely recognized in households, offices, public services, industries, etc. facing issues of security and privacy, concerns are leading causes for concern at IOT's service. Because of the many energy constrains and requirements along with power restricted battery, real-time execution etc., traditional cryptography algorithms will not match perfectly in the IOT platform. Lightweight cryptography is therefore more consistent with the IOT world. There are numerous LWC algorithms available they are, the symmetric and asymmetric algorithm, unfortunately these LWC algorithms cannot achieve real-time usage, execution time, energy utilization and memory specifications any assurance of security. There is no verification in symmetric algorithms, while asymmetric struggles from its greater key size and more power use. This influences the collecting and storing of data in real time and wasting IOT energy.

5. Counter Measures In IOT

5.1 Symmetric lightweight algorithms for IOT

a) AES

There are multiple models of Rijndael encryption, AES-128, AES-192 and AES-256, according to NIST. This can be offering a solution in CoAP (Constrained Application protocol) in the application layer. The encryption operation consists of a 4-part (4x4) matrix of 128-bit segments [17]. Sub byte, shift rows, mix column, and add round key coordinate the internal state.

b) TWINE

It uses the Feistel design that calls sub-key process 8 times per round and XOR and adds 4(4x4) S-box. In comparison to CLEFIA and HIGHT, to speed up diffusion, TWINE is permutation that is more complicated and combination. Within TWINE, to split all sub-blocks, permutation takes just half as many rounds as the circular change for a single sub-block gap.

c) High Security and Lightweight(HEIGHT)

For Feistel network, height requires very simple and basic activity. During the phases of encryption and decryption, this key is created. Lee et al. suggested a concurrent architecture involving fewer resources, a limited number of code lines and enhancing the RFID framework [18]. HIGHT is prone to saturation assault.

d) PRESENT

This is based on the SP network and is made up of 31 rounds PRESENT [19] is used for security purposes as a lightweight algorithm. It has a 64-bit block and two 80-bit and 128-bit keys [20]. This extended to the replacement layer, which requires 4-bit input, output of the S-box, for hardware implementation.

e) RC5

Rivest first used this for data-independent rotations [21]. It possesses the structure of Feistel and can function just as well as Lightweight algorithm used in scenarios for wireless sensors. RC5 is known to be w / r / b, where w implies the length of the term, r refers to the amount of transitions, and b refers to number of bytes usable in the text. It usually would function on scale of 32 bits but its versions can be 16, 32, 64. Use 0,1, .. 255 key bytes, it can operate with 0, 1, 255 rounds, default key length is 16 bytes on 20 operating rounds. It becomes susceptible to attack by differentials [22]. Below Table gives summary of symmetric LWC algorithms in IOT.

Table 2: Symmetric LWC Methods in IOT

Algorithms	Code Length	Structure	# Rounds	Key size	Block size	Feasible Attacks
AES	2606	SPN	10	128	128	Middle-in-man attack
HEIGHT	5672	GFS	32	128	64	Saturation attack
TEA	1140	FEISTEL	32	128	64	Related key attack
RC5	-----	ARX	20	16	32	Differential attack
PRESENT	936	SPN	32	80	64	Differential attack

5.2 Asymmetric lightweight algorithms for IOT

a) RSA (Rivest–Shamir–Adleman)

It operates by choosing two broad prime numbers to create the public and private key pairs [23]. Due to its large key scale, RSA does not belong to the lightweight cryptographic scheme. Public key is freely released although private key is kept safe. A little more efficient RSA protocol is introduced, which data are encrypted and decrypted to preserve user privacy [24] [25]. RSA provides greater protection and device privacy due to the use of two huge prime numbers and device service.

b) ECC (Elliptically Curve Cryptography)

ECC needs a smaller key length compared with the RSA algorithm. As such, speed of operation, which needs less power. It is extended to occupy the less area of hardware deployment, resulting in quicker real-time computation [26]. 6LoWPAN nodes use the ECC algorithm that could be extended to devices that are constrained. Bit changing is used to maximize minimal power device usage rather than using microprocessor activity for multiplication [27]. Below Table gives summary of asymmetric LWC algorithms in IOT.

Table 3: Asymmetric LWC Methods in IOT

Algorithm	Key Size	Code Length	Feasible Attacks
RSA	1024	900	Modulus Attack
ECC	160	8838	Timing Attack

6. Research Problem

Nowadays IOT acknowledges in households, offices, social areas or in industry companies that opens up the door to problems in security and privacy. Therefore, these problems make it huge concerns of IOT activity. The sum of damage that may arise is influential when predicting whether an assault is introduced into IOT. Multiple IOT attacks exist, such as eavesdropping, spoofing, Denial of Service (DoS), replay attacks, injection of false signals. Such threats would like to destroy IOT's safety services such as encryption, honesty, and authentication; in fact, it will affect user privacy. IOT offers all levels of advanced basic security solutions that are still vulnerable to attacks. Because of its limited resources like strength, real-time execution, In IOT case, conventional encryption and authorization systems do not fit well. Therefore, lightweight approaches to cryptography strive to function excellent on IOT. List of lightweight cryptography algorithms Symmetric and Asymmetric occur in literature such as AES, HIGHT, RC5, PRESENT, RSA, ECC and many more. Owing to more execution time, code duration, and memory constraints, these current technologies may not assure an optimum level of real time communication protection. The execution time takes more space to and the key management delivery, encryption and decryption, which defines protocol's effectiveness.

Because of their broad key size, asymmetric algorithms are sluggish, although symmetric algorithms could only provide confidentiality and honesty, authentication will not add to the availability challenge. That can have an impact the gathering and storing of data in real time, and IOT funds will start spending. It asks a secure IOT algorithm, which will in optimal time assurance services such as confidentiality, integrity and authentication.

7. Proposed Idea

Several scholars have suggested lightweight symmetrical and asymmetric protection algorithms for IOT based on literature survey conducted. Symmetric algorithms have confidentiality honesty, fewer key lengths, but are smaller difficult but not to provide reliability and key distribution is a challenging task in them. Asymmetric algorithms have confidentiality honesty, and reliability, yet their key length is too big to make them more complicated and not appropriate for restricted IOT scenarios.

Therefore, the need arises for a reliable algorithm built to chart the finest aspects of lightweight symmetric and asymmetric algorithms that require less time to implement maximum energy requirements and maintain anonymity, honesty and authenticity for all security services.

8. Conclusion

We have gone into detail in this paper about lightweight cryptographic algorithms. Many devices with low resources in an IOT world execute computations. In terms of memory, battery life, energy consumption and computations, these devices are limited. IOT systems still face security and privacy issues as well as the problem of how IOT consumers should retain trust. In addition, we have described various types of LWC algorithms are simple to help for deployment of hardware and firmware. Many traditional cryptographic algorithms are prone to certain types of intrusions that can mentioned in this paper as well. It is necessary to expand reliable LWC algorithms with lesser key size, faster computation and fewer processing power. We should look into how effective these approaches are in the future and whether they can be introduced in a restricted area.

References

[1] D. Singh, G. Tripathi, and A.J. Jara. A survey of Internet-of-things: Future vision, architecture, challenges and services. In *Internet of Things (WF-IOT), 2014 IEEE World Forum on*, pp. 287-292.IEEE, 2014.

[2] J. Bradley, J. Barbier, and D. Handler. Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience CISCO Whitepaper. White Paper, Cisco Systems Inc (2013).

[3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, Context Aware Computing for The Internet of Things: A Survey IEEE Communications Surveys & Tutorials, 2013, pp. 1-41.W Diffie, Multi-user cryptographic techniques, p. 50, 08 June 1976..

[4] W Diffie, Multi-user cryptographic techniques, p. 50, 08 June 1976.

[5] N Nurseitov, M Paulson, R Reynolds, and C Izurieta, Comparison of JSON and XML Data Interchange Formats: A Case Study, in *CAINE*, 2009, pp. 157-162.

[6] R M. Vucinic, Grenoble Alps Univ., Grenoble, France Grenoble Inf. Lab., B. Tourancheau, F. Rousseau, and A. Duda, OSCAR: Object security architecture for the Internet of Things, in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium*, Sydney, NSW , June 2014, pp. 1 - 10.

[7] K Islam, Weiming Shen, and Xianbin Wang, Security and privacy considerations for Wireless Sensor Networks in smart home environments, *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on* , p. 627,May 2012. [Online]..

[8] Roy T. Fielding et al. (1999, June) Hypertext Transfer Protocol -- HTTP/1.1. [Online].

[9] E. Rescorla, T. Dierksv, and Inc RTFM, The Transport Layer Security (TLS) Protocol Version 1.2, Internet Engineering Task Force (IETF), Standards Track RCF5246, March 2008. [Online]..

[10] Z. Shelby, ARM, K. Hartke, C. Bormann, and Universitaet Bremen TZI, The Constrained Application Protocol (CoAP), Internet Engineering Task Force (IETF), Standards Track 2070-1721, June 2014. [Online].

[11] R. Khan, Univ. of Genova (UNIGE), Genova, Italy DITEN Dept., S.U. Khan, R. Zaheer, and S. Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in *Frontiers of Information Technology (FIT), 2012 10th International Conference*, Islamabad, 2010, pp. 257 - 260.

[12] E. Rescorla, Inc. RTFM, N. Modadugu, and Inc. Google, Datagram Transport Layer Security Version 1.2, "Internet Engineering Task Force (IETF), PROPOSED STANDARD 2070-1721, 2012..

[13] L. Xiao-Wei:- Wireless Sensor Network technology, Beijing Institute of Technology press, pp.241-246 (2007).

[14] Z. Young-Bin and F. Deng-Guo: Design and analysis of cryptographic protocols for RFID, Chinese Journal of computers pp.583-584 (2006).

[15] Q. Gou., L. Yan., Y. Liu and Y. Li, Construction and strategies pm green computing and communications and IEEE Internet of Things and IEEE Cyber, pp.1129-1132 , (2013).

[16] C. Perera., A. Zaslavsky., P. Christen and D. Georgakopouls: Contextaware computing for the internet of things, A Survey, Communications surveys tutorials, IEEE vol 16, No 1 pp 414-454(2013).

[17] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. Cryptographic Hardware and Embedded Systems–CHES. Vol. 3156. 2004. p. 357–70.

[18] Lee JH, Lim DG (2014) Parallel architecture for high-speed blockcipher, HIGHT. International Journal of Security and its Applications 8(2):59–66.

[19] Nyberg K. Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. 2015. p. 165-85

[20] Bogdanov A, Knudsen L.R, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. Present: An Ultra Lightweight Block Cipher. Berlin Heidelb: Springer; 2007. P.0 450–66.

[21] Gawali DH. Rc5 Algorithm: Potential cipher solution for security in Wireless Body Sensor

Networks (WBSN).Int J Adv Smart Sens Netw Syst. 2012; 2(3):1–7.

[22] Biryukov A, Kushilevitz E. Improved cryptanalysis of RC5. Advances in Cryptology—EUROCRYPT'98. Vol. 1403. 1998. p. 85–99.

[23] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.

[24] Zhou X, Tang X. Research and implementation of RSA algorithm for encryption and decryption. Proceedings of 6th International Forum *Strategic Technology* (IFOST); 2011. p. 1118–21.

[25] Jamgekar RS, Joshi GS. File encryption and decryption using secure RSA. Int J Emerg Sci Eng. 2013; 1(4):11–4.

[26] Eisenbarth T, Kumar S (2007) A survey of lightweight-cryptography implementations. IEEE Design and Test of Computers 24(6):1–12.

[27] Ayuso J, Marin L, Jara A, Skarmeta A. Optimization of public key cryptography (RSA and ECC) for 16-bits devices based on 6LoWPAN. 1st International Workshop on Security Internet Things. Tokyo, Japan; 2010. p. 1–8.