A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs

Isha Bhardwaj
Electronics and Communication Department
Thapar University
Patiala, India.
bhardwaj.isha1804@gmail.com

Ajay Kumar
Electronics and Communication Department
Thapar University
Patiala, India.
er.ajay.thapar@gmail.com

Manu Bansal
Electronics and Communication Department
Thapar University
Patiala, India.
mbansal@thapar.edu

***Abstract*- Internet of Things (IoTs) comprises of a cluster of resource constrained devices, sensors and machines connected with each other and communicating over the internet. Due to frequent exchange of confidential data over the internet, IoTs become susceptible to various attacks (such as eavesdropping, denial of service, fabrication attacks) and to resolve these attacks security is required. In this paper, a brief discussion on the various IoT applications and architectures has been done. Further, the security concerns regarding information sharing and attacks have been highlighted. To overcome from these attacks safety measures regarding data security and authentication are discussed in detail resulting in use of cryptography as a solution. The comparative analysis of various lightweight encryption and authentication algorithms is carried out. The comparative analysis results show that the lightweight algorithms have good performance as compared to conventional cryptography algorithm in terms of memory requirement, their operations, and power consumption. Also, some research directions defined in which further work can be done on lightweight cryptography algorithms.**

Keywords- IoT Architectures, Attacks, Cryptography, Internet of Things, Lightweight Ciphers, Security.

I. INTRODUCTION

The forthcoming era of pervasive computing will be characterized by many smart devices [1]. One of the implementation of smart devices is Internet of Things (IoT). Internet of Things refers to unique objects which can interact and communicate information with other objects through wired or wireless medium. The IoTs are real time system which takes the data through sensors communicate in the network and provides facility to users to access, share and according to their requirement takes action. With the development of wireless sensor networks, inventions have been made in IoTs. IoTs have paved their way in day to day life of humans. The few applications of IoTs are mentioned below [2].

- Home automation system where one can control the electronic items in their house via their mobile phones and laptops thus creating a system that enables a smart home. It also provides the facility of detecting emergencies; maintain energy consumption inside the house, *etc*.
- Intelligent Transportation System in which traffic monitoring can be done, accidents, traffic jams and violation of traffic rules can be reported to authorities.
- Prediction of natural disasters and reporting critical temperature changes, by constant monitoring of environment using sensors. Monitoring Environmental pollution like measuring level of toxic gases in air, content of toxic material in water.
- Healthcare facilities can be provided like remote monitoring of patients, constant monitoring of health parameters and activities, support for independent living, monitoring medicines intake by the patient and many more.
- Surveillance and tracking of people, objects and animals, investigating spaces and deserted areas, maintenance of infrastructure and equipment, alarming systems and many more facilities have become possible with IoTs.

1.1 Overview of IoT Architectures

IoT does not only establish a connection between other objects for information sharing, it makes multiple decisions after network establishment. These decisions are taken in real time. This is accomplished through the architecture of IoT. In this section various architectures of IoTs are discussed.

- Three-layer Architecture

The Authors in [3] discuss the basic three layered architectures for IoT. The layers are called Physical layer, network layer and application layer from bottom to top. The Physical layer identifies everything in the IoT system. It gathers information about each object in the vicinity of the IoT. This layer contains RFID tags, sensors, cameras, etc, devices which help in collecting the information. Next layer is the Network Layer, it is also known as the core of IoT, and its work is to transmit information congregated by the physical layer. It contains all the software and hardware compositions of the network and is the management and information centre. The third layer of this architecture is the Application Layer. The target of this layer is to act as a bridge between industrial technology and social needs of IoTs.

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

The three-layer architecture gives basic level information but does not completely explain IoTs detailed structure and association.

- Four-Layer Architecture

Authors in [4] describe the four layered architecture of IoT and claim that it is the most appropriate model. It comprises of four layers, perception, heterogeneous network access, data management and intelligent service layer. It is easy to trade information between physical world and the cyber world through this architecture. Data Perception Layer is similar to Physical layer. Heterogeneous Network Access Layer has access to Internet universally via a wide range of wireless medium, mainly WiFi, Bluetooth, WiMAX, Zigbee, GSM, WCDMA and Satellite. Data Management layer manages data coming and going. There are centers for cloud computing, directory management severs, which help in storing data. The top layer called as Intelligent Service Layer provides intelligent services for the IoT users covering areas like agriculture, home automation, environment, transportation and so on.

- Five-Layer Architecture

After this 5-layer architecture was projected, starting from business layer, application layer, processing layer, network and perception layer. The Business layer is used to define the IoT applications and their management. Application Layer targets in determining the types of applications used in the IoTs. It also develops these applications, making them more smart, authenticated and safe. Processing Layer is responsible for handling the data congregated by perception layer. This process has two main features; analyzing data and storing it. The work of this layer is tough as it deals with huge amount of data. Therefore, it uses some techniques such as database software, cloud computing, ubiquitous computing, and intelligent processing in the processing of data and its storage. Network layer's purpose is to transmit and receive data back and forth from the perception to the processing layer. It uses technologies like infrared, Wi-Fi, and Bluetooth. Network layer addresses each thing in the system using IPV6. Perception Layer gathers the information from the vicinity of the system and converts this data into signals. It uses technologies like RFID and the GPRS to gather the information [5]. Apart from this IoT architecture should be apt enough to support all the features for its best possible use. The architecture should be capable to provide application support, Quality of Service, security and data management, and reliability, be resilient to attacks and have optimized performance. TABLE 1 gives the key features of different architectures in IoTs.

Table 1 Overview of IoT Architectures

3 Layer	4 Layer	5 Layer
Physical/Perception Layer Smart cards, RFID Tags, Sensors	**Data Perception Layer** RFID tags, 3G Phones, Sensor Embedded Devices	**Perception Layer** Physical Objects, RFID, Barcode, Infrared Sensors.
Network Layer Secure Transmission, 3G, UMTS, WiFi, Bluetooth, Infrared, Zigbee	**Heterogeneous Network Access Layer** Wireless links, GSM, WCDMA, WiFi, Zigbee	**Network Layer** 3G, WiFi, Bluetooth, Zigbee Infrared Technology
	Data Management Layer Cloud Computing Centers, Web service servers, management servers	**Processing Layer** Database, Ubiquitous Computing, Service Management, Info Processing
Application Layer Smart Applications and Management	**Intelligent Service Layer** Intelligent Applications as in agriculture, environment, smart cities etc	**Application Layer** Intelligent systems, devices, Applications in various domains
		Business Layer Business Models, Graphs, System Management

1.2 Attacks on IoTs

Communications in IoTs happen via Internet, which is a publically available network. This makes it susceptible to various attacks which cause interruption in smooth working of IoTs. Few attacks are discussed below

Denial of Service Attack (DOS): This attack stops the services of the network for authorized users as unauthorized users try to connect to that network. DOS in Physical Layer causes Jamming (the channel used for communication between the nodes is occupied by unauthorized party), node tampering (sensitive information is extracted by physical tampering of the nodes). On network layer DOS attack causes spoofing (a useless message is sent by a malicious node which is then replayed by the attacker to generate a high traffic) [6].

- Wormhole**:** This DoS attack causes rearrangement of bits of data from its original position in the network. An attacker records bits at one location in the network, channels them accordingly to another location, and then retransmits them there into the network [7].
- Man-in-Middle: In this attack an intermediary user gets the key of one of the communicating party and starts exchanging information as if it is the valid

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

party. It is a dangerous attack, the attacker fakes as the original sender. The attacker can trick the recipient into thinking they are still getting a correct message. RFID technology faces this type of attack the most.

- Eavesdropping: This attack is on the confidentiality as the intruder gets hold of the data being shared between sender and receiver. The other devices can constantly monitor data of the compromised device and can also transmit false messages to gather personal data of that device [8].
- Alteration: Information handled by IoT devices can be altered or modified by attackers causing threats to the integrity requirements of IoT system. Attackers do this to mislead the communication protocol.
- Fabrication: Here the attacker causes unauthorized insertion, modification of data into the IoT system. This causes threat to the authentication of the system as the sender has no knowledge that the system is compromised [9].

1.3 IoT Security Challenges

In section III the attacks on IoT network is discussed so to keep all connected devices secure security required. The IoT security classify in 3 ways. These are

- Security and Data Protection: Since IoT devices are wireless and share sensitive information on public networks they become vulnerable malicious attacks and information theft. It requires advance technology to secure the system [10]. Cryptographic algorithms are a good method to ensure information security in the IoT. But still many IoT devices are not powerful enough to support such robust techniques. Therefore, to enable them on the IoT, algorithms need to be less energy consuming, but should not compromise on their efficiency [11].
- Authentication and Identity management: It is an important constituent of any security model. Each object in the IoT network should be able to identify other objects and authenticate them. Unique identifiers can be used create personal identities of these objects. It ensures the identity of smart objects before any communication is done between them. A mechanism which enables devices to mutually authenticate before every interaction is very essential for the success of IoTs [12].
- Privacy: As objects are becoming traceable through IoT, privacy related threats have increased manifold. Securing data is important so it is not misused by any third person. Despite this, issues related to data ownership should also be addressed. In order to make the user feel comfortable in being part of the IoT system measures must be taken. The ownership of the information collected from different smart objects must be distinctly established. The owner must be guaranteed that the data will not be used without their consent, specifically when it will be shared over the internet [13]. Privacy of information can be ensured via Privacy Policies. Smart devices can be equipped with these policies. Therefore, when the smart objects come into contact with each other, they can go through their respective privacy policies for compatibility before communicating any information [14].

1.4 Overview of Cryptography for IoTs

There can be various solutions at the respective layers of IoTs used in the end to end communication. The cryptography algorithms are taken for data security. Cryptography is a technique in which we can encrypt data into cipher text for its secure transmission. Cryptographic ciphers are of two types, symmetric and asymmetric ciphers. Symmetric key encryption uses same key for both encryption and decryption of data. This method of encryption is extremely secure and relatively fast. The major disadvantage of symmetric key encryption is sharing of the key between the communicating parties. If the key gets in hands of some malicious party, then the encrypted data gets compromised. Symmetric key algorithms assure confidentiality and integrity of data, but do not guarantee authentication. Some of the traditional symmetric key ciphers are AES, DES, 3DES, BLOWFISH, IDEA, [15] etc. Asymmetric key encryption uses two keys, private and public key for communication between the sender and receiver. Asymmetric encryption provides authentication, confidentiality and integrity. To ensure confidentiality and Integrity the sender uses public key for encryption of data and the receiver uses his private key to decrypt it. To guarantee authentication, sender uses his private key for encryption data and receiver confirms it by decrypting it with public key of sender [15]. The advantage of asymmetric cryptography is it supports all security services and also provides a safe mechanism for key sharing. The only limitation it has large key size which makes encryption slow and increases the complexity. The most common algorithms used are RSA by Rivest, Shamir and Adleman, Deffie-Hellmen key exchange (DH), Elliptic Curve Cryptography (ECC).

The IoT devices such as RFID, smart cards, sensors nodes play an important role in the network. These devices have limited memory and are battery operated devices. The standard cryptography algorithms (such as AES) provide good security but their performance is not acceptable on these devices because of large memory requirements to store s-boxes, large block and key sizes. To resolve these issues, NIST recommended preferring lightweight algorithms which provide same level of security and their performance is also acceptable on these devices [16].

II. Literature Survey on Lightweight Cryptography Algorithms for IoT Security

In this section a survey on lightweight cryptography algorithms is done. Based on it comparison of ciphers is shown. It gives way to research directions in which further work can be done.

The lightweight cryptography algorithms are designed keeping AES as standard **AES** (Advance Encryption Standard) algorithm, because it's standardized by NIST. It is a symmetric block cipher, works on the block length of 128 bits with variable key sizes of 128, 192, 256 bits. It is based on substitution permutation network (SPN) and works on 4*4 matrixes. Every byte gets affected by sub bytes, shift rows, Mixed Columns, Add Round Key [17, 18]. **PRESENT** is also based on SPN structure. It is one of the ultra-lightweight algorithms used for security. It has key size of 80 or 128 bits and operates on blocks of 64-bit [19]. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. The PRESENT algorithm is hardware efficient but permutation layer of PRESENT cipher consumes large cycles in software level so an improved version of PRESENT algorithm was proposed known as RECTANGLE cipher. **RECTANGLE** [20] is a bit-slice ultra-lightweight block cipher suitable for multiple platforms that have very low area in hardware and also very competitive performance in software. RECTANGLE has SPN structure; it supports 64 bits block size, 80 or 128 bits key size with 25 rounds**. High security and lightweight (HIGHT)** is based on Feistel Network structure. It uses basic operations like addition mod 2^8or XOR. It has a block size of 64-bits and works with 128-bit key, with 32 rounds [21, 22]. **CLEFIA** is another lightweight cipher that was standardized by NIST in 2007. It is based on Feistel Network. It supports a block size of 128 bits and key lengths of 128, 192 and 256 bits. CLEFIA is a well-balanced block cipher in performance and security. It has good hardware performance in comparison to other block ciphers [23, 24]. **CAMELLIA** is a symmetric key block cipher which has a block size of 128 bits and works with 128, 192 and 256-bits keys respectively. It was designed for both software and hardware implementations. It can be used for low cost smart cards to network systems with high speeds. It is used in Transport Layer Security [25, 26] a cryptographic protocol which was designed to provide security over a computer network like internet. **TWINE** [27, 28] fits in very small hardware and provides a notable performance on embedded software. TWINE is generalized Feistel Structure of type 2 with a highly diffusive block shuffle. TWINE has two types, TWINE−80 and TWINE−128 with their respective key sizes. Both algorithms have 64 bits block size and 36 rounds. Each round of TWINE involves a nonlinear substitution layer using 4-bits S-boxes and a diffusion layer which permutes the blocks (4 bits). This round function is iterated 36 times for both key lengths. **SIMON** and **SPECK** were introduced in June 2013. Simon is a lightweight cipher which is optimized for performance in hardware implementations, whereas Speck has been optimized for software implementations [29]. TABLE 2 shows the comparison of various lightweight ciphers based on their key, block size and rounds, structure, performance parameters, merits and their attacks.

Table 2 Comparative Analysis of Lightweight Ciphers for Encryption

Ref.	Algorithm	Key Size (bits) Block Size (bits) Rounds			Structure	Performance				Merits	Attacks/Analysis
						Tech. (µM)	Power (µW)	Area (GE)	Throughput At 100Khz (Kbps)		
[17]	AES	128	128	10	SPN	0.13	2.48	2400	56.64	Supports larger key sizes, faster in both hardware and software.	Related key attack, Boomerang, Biclique cryptanalysis
[19]	PRESENT	80	64	32	SPN	0.18	1.54	1030	12.4	Ultra Lightweight cipher, Energy efficient.	Integral, Bottleneck attacks, truncated differential cryptanalysis, Side-channel attacks
		128				0.18	2.00	1339	12.12		
[20]	RECTANGLE	128	64	26	SPN	0.13	1.78	1787	246	Fast implementations using bit slice techniques	slide attack, related-key cryptanalysis, statistical Saturation Attack
[22]	HIGHT	128	64	32	FN	0.25	5.48	3048	188.20	Ultra-lightweight, provides high security, good for RFID tagging.	Impossible differential attack on 26th round, Biclique cryptanalysis

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

[23]	CLEFIA	128	128	18	FN	0.13	2.48	2488	39	Has fast encryption and decryption, lesser rounds, energy efficient	Key Recovery Attack on 10th round, Saturation Cryptanalysis
[26]	CAMELLIA	128	128	18, 24	SPN	-	1.54	6511	290.1	Resistance to brute force attack on keys, security levels comparable to AES.	Cache timing attacks , Impossible differential attack
[28]	TWINE	80, 128	64	36	FN	0.09	1.30	1866	178	Good for small hardware, efficient software performance	Meet-in-the-middle attacks, Saturation Attack
[29]	SIMON	128	128	64	SPN	0.13	1.32	1317	22.9	Supports several key sizes, performs well in Hardware	Differential fault attacks, Attacks on reduced versions
[29]	SPECK	128	128	32	SPN	0.13	1.40	1396	12.1	Performs better in software	Key Recovery, Boomerang attack

The TABLE 2 reflects that PRESENT, SIMON and SPECK have low gate area which is suitable for IoTs. The algorithms which are based on Feistel networks use same hardware for encryption and decryption i.e. the functions are reversible; this reduces memory and execution time.

In case of asymmetric ciphers **ECC** is best known lightweight cipher among them. It has less key size when compared to RSA algorithm. It has less memory requirements and increased computation speed. ECC has proved to be stronger against various attacks in wireless sensor networks and many other wireless suitable environments. It provides the same level of security in a 160-bit key size when compared to security provided by 2048-bit key size of RSA [30]. **RSA** generates public and private keys using two large prime numbers which makes it more secure. ECC uses discrete logarithmic problem to generate keys. Asymmetric ciphers are known to provide data authentication therefore they can be used in Digital Signature schemes to secure communication line [31]. TABLE 3 shows comparison between RSA and ECC based on their key size, key generation, signature generation, verifications, merits and their attacks. The Table shows ECC has better performance and provide high security than RSA when large key size is used. So, in the modern era for authentication purposes ECC will be preferred over RSA in IoTs.

III. Future Direction

From the survey and comparative analysis, the following research issues are found on which further work can be done.

- In IoT, data security and authentication is a big concern so numbers of techniques are proposed in which hybrid models of encryption and authentication algorithms are made (such as hybridization of AES and RSA technique) but this causes increase in the memory requirement on the devices. To counter this problem, the encryption algorithms are worked in CCM mode which provides security as well as authentication.
- In the lightweight cipher to provide the same level of security as in conventional cipher, the number of rounds increased. The large number of rounds degrades the performance. So, the future research direction is design lightweight cipher such as way that it provides fast confusion and diffusion in less number of rounds.

Table 3 Comparative analysis of Lightweight Asymmetric Algorithm for Authentication

	Algorithm	**Key Size (bits)**	**Key Generation(s)**	**Signature Generation(s)**	**Signature Verification(s)**	**Merits**	**Attacks**
[34]	RSA	1024	0.16	0.01	0.01	Increased security	Man-in-the-middle, Timing, Factoring attacks
		15360	679.06	9.20	0.03		
[34]	ECC	163	0.08	0.15	0.23	Increased speed, less memory requirement, optimum security level	Side channel attacks
		571	1.44	3.07	4.53		

978-1-5090-5838-9 /17 $31.00 © 2017 IEEE

- The RSA and ECC algorithms mathematical modeling based on discrete logarithm and modular arithmetic. These modeling include large number of multiplication operation. So, research direction is to use Vedic Multiplier (such as UT and NDD Vedas) in place of conventional multiplier for fast response.

IV. Conclusion

Internet of Things has been rapidly finding its path through our modern-day life and is aiming to improve the quality of life by connecting us with many smart devices, technologies, and applications. The IoT will create a scenario of complete automation of everything around us. Although a lot of research has been done in the IoT, but still there is more to explore in it. The rising attention of industries and governments in this technology has led to a wide spread research and resulted in many successful projects. Some of the challenges in IoTs like the overall architecture, security and privacy concerns have drawn a lot of attention, while others concern like availability, reliability, and performance of the smart devices still require more consideration. In this paper we discussed about the different architectures, security, privacy issues and lightweight solutions that can be taken to solve them.

Acknowledgement

The authors are grateful to DeitY for the financial support through 'Visvesvaraya Fellowship' and 'SMDP chips to System Design' project. The authors also want to express their sincere gratitude towards the Director, Thapar University, Patiala for his persistent support and encouragement.

References

[1] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *Ninth International Conference, on Computational Intelligence and Security,* Dec. 2013, pp. 663-667.

[2] R. Khan et al., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *10th International Conference on Frontiers of Information Technology,* Dec. 2012, pp. 257-260.

[3] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," in *Computer Communications,* 54, pp.1-31.

[4] O. Said and M. Masud, "Towards Internet of Things: Survey and Future Vision," in *International Journal of Computer Networks,* 2013, vol. 5(1), pp. 1–17.

[5] M. Wu et al., "Research on the architecture of Internet of Things," in *3rd International Conference on Advanced Computer Theory and Engineering*, 2010, pp. 484-487.

[6] P. Shah et al., "Applications and Challenges Faced by Internet of Things - A Survey," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Future Intelligent Vehicular Technologies,* Springer, 2017, pp.182-188.

[7] Y.C. Hu, A. Perrig and D. Johnson, "Wormhole attacks in wireless networks," in *IEEE Journal on Selected Areas in Communications*, 2006, vol. 24(2), pp. 370-380.

[8] Q. Xaio, T. Gibbons and H. Lebru, "RFID Technology, Security Vulnerabilities, and Countermeasures," in *Supply Chain the Way to Flat Organization,* Intech, 2009, pp. 357-382.

[9] M. Nawir et al., "Internet of Things (IoT): Taxonomy of security attacks," in *3rd International Conference on Electronic Design,* Phuket, 2016, pp. 321-326.

[10] A. Whitmore et al., "The Internet of Things—A survey of topics and trends," in *Information Systems Frontiers,* Springer, April 2015, vol. 12(2), pp. 261-274.

[11] D. Bandyopadhyay and J. Sen, "Internet of Things: applications and challenges in technology and standardization," in *Wireless Personal Communications*, Springer, 2011, vol. 58(1), pp. 49–69.

[12] P. Mahalle et al., "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges," in *Recent trends in network security and applications, communications in computer and information science*, Springer, 2010, vol. 89, pp. 430–439.

[13] R. Roman et al., "Securing the Internet of Things," in IEEE Computers, 2011, vol. 44(9), pp. 51–58.

[14] T. Borgohain et al., "Survay of Security and Privacy Issues of Internet of Things," in *International Journal of Advanced Network Applications,* 2015, vol. 6(4), pp. 2372-2378.

[15] K. Acharya et al., "Analysis of Cryptographic Algorithms for Network Security," in *International Journal of Computer Applications Technology and Research,* 2013, vol. 3(2), pp. 130-135.

[16] T. Eisenbarth et al., "A Survey of Lightweight-Cryptography Implementations," in *IEEE Design & Test of Computers,* 2007, vol. 24(6), pp. 522-533.

[17] A. Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," in *Advances in Cryptology – EUROCRYPT 2011 Lecture Notes in Computer Science,* Springer, 2011, vol. 6632, pp. 69-88.

[18] M Feldhofer et al., "Strong Authentication for RFID Systems Using the AES Algorithm," in *Cryptographic Hardware and Embedded Systems – CHESS 2004 Lecture Notes in Computer Science,* Springer, 2004, pp. 357-370.

[19] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007 Lecture Notes in Computer Science*, Springer, 2007, pp. 450-466.

[20] W. Zhang et al., "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in *Science China Information Sciences,* 2015, vol. 58(12), pp. 1-15.

[21] H. Yap et al., "EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption," in *Cryptology and Network Security Lecture Notes in Computer Science*, Springer, 2011, pp. 76-97.

[22] D. Hong et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device," in *Cryptographic Hardware and Embedded Systems - CHES 2006 Lecture Notes in Computer Science,* 2006, pp. 46-59.

[23] T. Akishita and H. Hiwatari, "Very Compact Hardware Implementations of the Blockcipher CLEFIA," in *Selected Areas in Cryptography Lecture Notes in Computer Science,*Springer, 2012, pp. 278-292.

[24] T. Shirai et al., "The 128-Bit Blockcipher CLEFIA (Extended Abstract,)" in *Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science*, Springer, 2007, vol.4593.

[25] Isha and A. K. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things," in *Indian Journal of Science and Technology,* 2016, vol. 9, pp. 28.

[26] A. Satoh and S. Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," in *Lecture Notes in Computer Science Information Security,* Springer, 2003, pp. 252-266.

[27] T. Suzaki et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," in *Selected Areas in Cryptography Lecture Notes in Computer Science,* Springer, 2013, vol. 7707, pp. 339-354.

[28] P. Kumarkushwaha et al., "A Survey on Lightweight Block Ciphers," in *International Journal of Computer Applications,* 2014, vol. 96(17), pp. 1-7.

[29] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers," in *Proceedings of the 52nd Annual Design Automation Conference,* 2015, pp. 1-6.

[30] D. Mahto et al., "Security Analysis of Elliptic Curve Cryptography and RSA," in *Proceedings of the World Congress on Engineering,* 2016, vol. 1.

[31] R. Sinha et al., "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography," in *International Journal of Scientific & Engineering Research,* 2013, vol. 4(5), pp. 720-725.