An Evaluation of Lightweighted Data Security and Authentication Schemes for IoT Devices

Shreyas Srinath[1]
Dept. of Computer Science
R.V College of Engineering
Bengaluru, India

Nagaraja G S[2]
Dept. of Computer Science
R.V College of Engineering
Bengaluru, India

Abstract

IoT devices are majorly challenged on processing cycles, battery power & network capabilities. IoT devices deployed in production systems and in research studies have major concern in data security & network security related issues. To address this, there are cryptographic security algorithms that takes more execution cycles and memory which are not suitable for a resource constraint IoT device. Light weight cryptographic algorithms are designed such that it should be able to work in resource constraint environment also to provide sufficient security while transferring data. The study on different light weighted cryptographic algorithms used in research and industry for IoT device, their timing analysis, comparative analysis with standard algorithm, recommendations are presented.

Keywords: - Authentication, Cryptography, IoT, Security

I. INTRODUCTION

Simple definition of IOT (Internet of Things) can be, it is connecting device to internet. Consider a simple example of an automation of home using IoT, here different sensors which gives various important data related to humidity, temperature, motion etc. are gathered and transferred to the server which is present on the cloud. This server will process the data and by using some statistical tool it will make some prediction which can be used to trigger any action or predicts an event based on the history data. Generally, the server is used to control all the sensors and devices which are involved in home automation. User or developer can access the server through internet and control the automated system from any place. Now the main issue here comes which is of high concern is security and authentication. Data needs to be protected from the third-party attacker or hackers. For these various algorithms are implemented but the microcontroller used in the IoT are of low power and has less memory capacity (RAM & ROM). It was found that traditional algorithms which were running on desktops or servers to make the secure data transmission requires more power and capacity which is not able to provide by this low power devices for example RSA Traditional data security algorithms are not feasible for IoT devices communication because of resource constraints of IoT Devices.

To address this problem, there is a need for light weighted data security algorithms which are secure and consumes less processing power for making secure device level end to end communication. Here light weight does not refer to weakness but it refers to that, this algorithm can be implemented with the lesser resource requirement such as we have in case low power device that is power and memory capacity.

II. Literature Review

Major factors affecting security of IoT are mentioned below

Scalability - The customization, scalability, and diversity is a major challenge to be addressed. Scalability is adaptability, how much capable a device is to adapt with the changing environment and as per the need in the future. It is able to handle the growing amount of task.

Diversity – The generic IoT security design is becoming challenging because of diversified IoT edge device platforms. More of the devices manufactured for IOT purpose do not have proper standardisation. Plus, it provides the internet connectivity which leads to security concern.

Device life - Device life can range from short to long, depending on the IoT applications. Data or physical device security techniques adapted needs to be designed depending on battery capacity. The battery provided should support IOT device as well as the processing part of it.

Open-source IoT systems - Open source architecture and software are widely used in IoT systems. The advantage of using open source is that the same modules fits in a sprawling range of other products. But the drawback is that the whole system will get compromised or comes to halt if hackers or the third party attack all the IoT edge nodes present in the IoT network.

Cloud Data center - All the business activity in IoT is carried out with cloud-based data storage. IoT with cloud are interlinked to operate it from any part of the geo. IoT includes sensors, actuators, and processing unit, out of these the sensor will be active most of the time which produces large data which is stored onto cloud. This storage of large data can result into alarming risk of security related issue.

Authentication and pairing - IoT network consist of many devices such as sensors etc. connect to each other forming a network. Each sensor may or may not be linked to each other. If they are linked to each other they would share data, this data needs to be encrypted, otherwise the hackers can tamper with this data. All sensors end nodes are interconnected so an adversary if affects a node can tamper all the other nodes connected to the network.

In Paper [1] Comparative analysis is made on the existing stimulation tools which are classified based on IoT architecture layers coverage. There come the challenges of currently used stimulators and testbenches that needs to be looked into by the team of IoT research group, to make an IOT simulation that is robust and effective and evaluate the prototype.

Lightweight Protocols - 6LoWPAN, uIP, RPL, nanoIP, TSMP.

Energy Efficient protocols - EnOcean, LoRa, IEEE 802.11ah, IEEE 802.11af, IEEE 802.11ba. Security perspective protocols - CLEFIA, PRESENT, ENOCORO, TRIVIUM

Some of the software compared in this paper are

Cooja – last release on 2017 - small scale network –opensource

Omnet++ - stable release 2019 - large scale networks – opensource

NS3 – release 2020 – large scale networks support for LoRaWAN- open source Linux based

QualNet- 9.0 release 2019 - 802.15.4 (ZigBee support) – Paid software –GUI based

In paper [2] the comparative analysis of various light weight cryptography algorithm is carried out and the result reveals that the performances of these lightweight algorithms are improved as opposed to traditional, cryptography algorithms, the metric of memory and power consumption are taken for consideration for comparison. Comparative analysis on different lightweight algorithms are tabulated as per table 1.The experimental results in the table 1 shows that the AES algorithm with a key size of 128 bits and block size of 128 bits performs the encryption in 10 rounds consuming power worth 2.48uW with a throughput of 56.64Kbps at 100Khz.The PRESENT algorithm with a key size of 80 bits and block size of 64 bits performs the encryption in 32 rounds consuming power worth 1.54µW with a throughput of 12.4Kbps at 100Khz.

Table 1: Comparison of performances of several lightweight algorithms used in IoT space

Algorithm	Key Size (bits)	Block Size(bits)	Rounds	Performance		Attacks
				Power (µW)	Throughput at 100Khz (Kbps)	
AES	128	128	10	2.48	56.64	Related key,Boomerang
PRESENT	128	64	32	1.54	12.4	Side channel attack
	128	64	32	2	12.12	
RECTANGLE	128	64	26	1.78	246	Statistical saturation attack
HIGHT	128	64	32	5.48	188.2	Biclique cryptanalysis attack

The PRESENT algorithm with a key size of 128 bits and block size of 64 bits performs the encryption in 32 rounds consuming power worth 2uW with a throughput of 12.12Kbps at 100Khz.The RECTANGLE algorithm with a key size of 128 bits and block size of 64 bits performs the encryption in 26 rounds consuming power worth 1.78uW with a throughput of 246Kbps at 100Khz.The HIGHT algorithm with a key size of 128 bits and block size of 64 bits performs the encryption in 32 rounds consuming power worth 5.48uW with a throughput of 188.2Kbps at 100Khz.

In comparison with the power consumption of AES algorithm that has 128 bits key length and 128 bits block length, the PRESENT algorithm consumes 0.008% less with 80 bits key length and 64 bits block length, the PRESENT algorithm consumes 0.48% less with 128 bits key length and 64 bits block length, the RECTANGLE algorithm consumes 0.7% less with 128 bits key length and 64 bits block length.

Table 2: Timing analysis of RSA and ECC applied for IoT device

Algorithm	**Key size (bits)**	**Key Generation (in sec)**	**Signature Generation (in sec)**	**Signature Verification**	**Attacks**
RSA	1024	0.16	0.01	0.01	Man, in the middle
	15360	679.06	9.2	0.03	
ECC	163	0.08	0.15	0.23	Side channel attacks
	571	1.44	3.07	4.53	

The experimental results shown in table 2 indicates that

RSA algorithm has two instances:

a. a. RSA algorithm for 1024 bits key size takes a time of 0.16s for key generation, 0.01s for signature generation and 0.01s for signature verification.

b. b. RSA algorithm for 15630 bits key size takes a time of 679.06s for key generation, 0.9s for signature generation and 0.03s for signature verification.

ECC algorithm has two instances:

a. ECC algorithm for 163 bits key size takes a time of 0.08s for key generation, 0.15s for signature generation and 0.23s for signature verification.

b. ECC algorithm for 571 bits key size takes a time of 1.44s for key generation, 3.07s for signature generation and 4.53s for signature verification.

In RSA algorithm, between the two key sizes, there is a difference of 6.79% for key generation, 0.008%for signature generation and 0.0002% for signature verification times.In ECC algorithm, between the two key sizes, there is a difference of 0.01% for key generation, 0.03%for signature generation and 0.04% for signature verification times.In concluding the previous two points, both RSA and ECC algorithms are inefficient with respect to IOT as difference in key size should not result in increase of time.

As security and authentication are critical concerns in IoT, many techniques are proposed such as hybrid implementation of AES (Advanced Encryption Standard) and RSA (Rivest, Shamir, Adleman) but implementations of this technique require large memory.

In paper [3] proposed an Intelligent Security Framework for IoT Devices . This projected method is comprised of

(a) Lightweight Asymmetric cryptography for securing the End To-End devices data flow. For protecting the IoT Services, low power sensor network nodes and the gateway,

(b) Implementation of a Lattice based cryptographic method to make a secure transaction on broker devices or gateway devices for the cloud infrastructure.

The author's proposed architecture implements session key for message transfer . Also, this session key is shared between nodes through asymmetric key encryption method

The system is then protected from, Quantum algorithm and eavesdropping attacks.

Eavesdropping, quantum attacks, and DDoS (Distributed Denial of Service Attacks) in IoT can be avoided using this technique.

Unique device identification (Did) of the sensor which is distinctive of each sensor is used to generate Kp (Key pair) by this protocol which will launch the mutual authentication in between services and IoT devices. Gateway, which joins the device and the cloud services, have the mutual authentication system for secure data and control transaction

In Paper [4] To secure the data light weight protocol is used. Data provenance is accessible for multihop IOT networks. link fingerprints are generated by RSSI (Received Signal Strength Indicator) which is the part of the communicating IO T nodes. By matching the ink fingerprints stored at the server, Correlation coefficient is calculated. The correlation coefficient percentage will determine the secured data transaction percentage. i.e., Higher the correlation coefficient higher is the data transferred in secured manner.

If the value of correlation coefficient is lower that means, in between a specific link, there is a presence of adversarial node. For data provenance to be achieved, all the link fingerprints available at the server is compared to the incoming packet header. Energy dissipation at each IoT node in the entire network is calculated.

The result is that power consumption for each IOT node is 52-53mJ for the system presented in this paper and 313.626mJ for the entire network as depicted in table 3.

Table 3: Power dissipation comparison for different fingerprints

Node	Fingerprints (bytes)	Transmission cost	AES-128 (µJ)	SHA-1 (µJ)	ECDSA-160 (mJ)	Total (mJ)
1	16	76.8	1.83	308	52	52.386
2	32	153.6	3.66	616	52	52.773
3	16	76.8	1.83	308	52	52.386
Total Energy dissipated						**157.545**

The experimental results from the table 3 imply that, 1st IoT node with a fingerprint size of 16 bytes incurs a transmission cost of 76.8uJ, AES-128 cost of 1.83uJ, SHA-1 cost of 308uJ, ECDSA-160 of 52mJ with a total cost of 52.386mJ.

The 2nd IOT node with a fingerprint size of 32 bytes incurs a transmission cost of 153.6uJ, AES-128 cost of 3.66uJ, SHA-1 cost of 616uJ, ECDSA-160 of 52mJ with a total cost of 52.773mJ.The 3rd IOT node with a fingerprint size of 16 bytes incurs a transmission cost of 7608uJ, AES-128 cost of 1.83uJ, SHA-1 cost of 308uJ, ECDSA-160 of 52mJ with a total cost of 52.386mJ. The total energy dissipated will be 157.545mJ.

In paper [5] End device encryption power issue of AES is addressed in this paper. Secured communication with low power consumption is proposed called LoRaWAN named as Secure Low Power Communication (SeLPC) method. During data encryption the power consumption reduction is the main motive to develop this scheme and is achieved by reducing the cycles of AES.

Simplified AES encryption with enhanced security level is been presented in SeLPC that makes the algorithm to consume less power.

Table 4: Power consumption for each cycle comparison

Power consumption of AES -128 and simplified AES				
AES -128			**Simplified AES**	
Encryption Step	**Round**	**Power (µW)**		
Add round key	11	17.3	6	9.5
Sub bytes	10	1883	5	941.5
Shift Rows	10	7.9	5	3.9
Mix Columns	9	1694.7	4	753.2
Total		3602.9		1708.1

The contents of Table 4 imply:

AES-128 with, add round key with 11 rounds consumes 17.3uW, SubBytes with 10 rounds consumes 188.3uW, ShiftRows with 10 rounds consumes 7.9uW, MixCloumns with 9 rounds consumes 1694.7uW of power amounting to a total of 3602.9uW of power consumed.Simplified AES with, add round key with 6 rounds consumes 9.5uW, SubBytes with 5 rounds consumes 941.5uW, ShiftRows with 5 rounds consumes 3.9uW, MixCloumns with 4 rounds consumes 753.2uW of power amounting to a total of 1708.1uW of power consumed.

Comparing this shows that simplified AES is 18.9% more efficient in energy saving than AES-128. As shown in the table 4, the presented SeLPC minimizes the encryption power by 26.2% as compared with traditional AES encryption method. Traditional LoraWAN consumes 345 milli Watt per day, proposed SeLPC dissipated 255.32 milli Watt for performing key update data encryption and checking message integrity.

In paper [6] SecureData is an IOT based data collection scheme, secured, for health care system as put forth by the authors. On the FPGA hardware, an optimized implementation is done. Secret cipher text method of transmission is implemented on the patient’s data to protect their privacy. Cloud computing layer for data privacy is been implemented to guarantee patients personal data [5]. FPGA simulations validate Secured Data performance in terms of, for all the algorithms, hardware frequency rate, energy cost, and computation time to show that secured data, when applied to protect security risks, is efficient for healthcare in IOT. The proposed algorithm takes around 1 second for encryption process and consumes around 80pJ /bit.

In paper [7] light weight algorithms are implemented on Arm CPU based implementation and ECDSA (Elliptical Curve Digital Signature Algorithm), light weight authentication technology is adapted for encryption. Test bench for the experiment is designed in 3 categories with different controller, OS with different frequencies.

Arduino due and RIOT	- 84MHz
MS500 and RIOT	- 96 MHz
MS500 and free RTOS	- 96MHz

Test results from the above experiments are tabulated in table 5 for comparative analysis.

Table 5: Operation time comparison of ECDSA signature and verification on different setups

Test Platform	Operating Time	
	ECDSA Sign (ms)	**ECDSA Verification (ms)**
Arduino due & RIOT	241	1222
MS500	274	1419
MS500 & free RTOS	202	1067

In paper [8] There is a protocol in latest ZigBee 3.0 for integration in protocol stack and IOT device constraint proposed by Lightweight Certificateless Key Agreement for Secure IOT Communication (LiKE). Lightweight cipher provides more security, by increasing the number of cycles but having a huge bulk of iterations reduces the efficiency and hogs the processing cycles of the cipher. So further research is to develop a lightweight cipher that provides security to the same extent as that of a standard cipher by restricting the increase of rounds.A hardware platform like OpenMote-b, with LiKe, requires 3.259s as a total time for establishing session keys. The overall capacity of the battery is 0.258%.

III. NIST 8114 Specification Lightweight Cryptography

When a new algorithm for secure data transmission is to be designed for IoT the NIST specification can be followed as NIST standards are designed to design any algorithm and put it on a general-purpose computer,

As per the specification below things can be incorporated while designing a new algorithm

Smaller block sizes: Smaller block sizes are allowed in lightweight which can be less than AES (like 64 bits or 80 bits, rather 128 bits). smaller the number of plain text blocks will reduce the limit of plaintext blocks to be encrypted

Smaller key sizes: A key size minimum of 112 bits is recommended by NIST.

Simpler rounds: S-Boxes of 4-bits are preferred over 8-bit for lightweight algorithm designs

Simpler key schedules: Simple key schedules are used by lightweight block ciphers that generates sub-keys on the go. This is prone to attacks like weak keys, related key, known keys or chosen key attack.

Minimal implementations: Necessary modules of a cipher which take lesser resources than implementing full cipher are advised.

IV. Research Gap identified from the literature review

In IoT, according to a study done by HP, 70% devices fall prey to attacks [9]. Man-in-the-middle attack is performed by sensing transmission between two nodes. Reliable solutions have been put forth to solve these attacks. However, Encryption may lead to minimal damage done to the integrity of the data. It is necessary for a security mechanism to be in place to assure unification of data when it is in transit as well as during its storage in the middle ware. Several algorithms in cryptography are developed to provide a solution but their utilization in IoT is uncertain as IOT's hardware is unsuited for implementing computationally affluent cryptographic algorithms [12]. A solution that can fulfil the need for security with a low computational cost must be found [28].

Cryptography algorithms are used for data security; It can be used to give solutions to the respective IOT layers that are used in end-end communication [10][11]. Cryptography is a technique which, for its secure transmission, encrypts data into a cipher message. Cryptographic ciphers are of two types; asymmetric and symmetric. In case of Symmetric key encryption, the same key is utilized for encrypting as well as decrypting data. This being a very secure and a relatively fast method of encryption. The key disadvantage of this method is that the key should be shared between the parties who are communicating. Compromise in the security of the key leads to the encrypted data also being compromised. Confidentiality and data integrity are assured in this algorithm, but not authentication. AES, DES, 3DES, BLOWFISH, IDEA, [15][13] etc. are traditional symmetric ciphers. Asymmetric encryption uses a separate private key and a separate public key for sending messages between the parties.

Authentication, integrity, and confidentiality are provided by encryption using asymmetric key. Using the public key, the sender encrypts the message to send and the receiver, using his private key, decrypts the message, this ensures confidentiality and integrity. The sender then uses his private key for encryption the message and the receiver, with the sender’s public key, decrypts it thereby ensuring authentication [15]. The advantages are that it all security services are supported and a safe platform, for key sharing, is provided [14]. Its bulky key size is the only drawback, which makes for complex and slow encryption. The commonly used algorithms are RSA, Deffie-Hellmen key exchange (DH), Elliptic Curve Cryptography (ECC). IoT devices like RFID tags, smart cards, sensors nodes perform a major part in a network.

These devices are battery operated and have limited memory. AES, a Cryptography algorithm, offer decent security solutions albeit with unacceptable performance as they need vast memory for storing s-boxes, large blocks as well as keys. NIST recommended, to answer these issues, the use of a lightweight algorithm that provides identical levels of safety and their performance is accepted on these gadgets [16].

V. Review Summary

Reviewing the study and its comparative breakdown, further issues in research were found to work upon.

• Data security and authentication are chief concerns in IOT, thus a number of procedures are planned where authentication algorithms and hybrid encryption models are formed, like hybridization of AES and RSA, merely this led to a growth in memory requirement on the gadget. As a counter, CCM mode runs the encryption algorithms which provide authentication and safety [17].

• In the lightweight cipher, to provide the same level of safety proffered by an orthodox cipher, the round number are hiked. The high number of rounds reduce performance.[20] Future development is a lightweight cipher that can be designed in a way that offers confusion and diffusion rapidly in minimal rounds. The RSA algorithm and ECC algorithm’s mathematical modelling are built on discrete logarithm and modular arithmetic. The models incorporate a great number of multiplication operations. So, further research can be done on using Vedic Multiplier, such as UT and NDD Vedas, in lieu of orthodox multiplier for quick response [19].

In all the above papers it is observed that, the proposed algorithms are making the communication secure in trade-off with the processing power utilization. Most of the battery of IoT device will be utilized in making the communication secure by running the algorithm, hence the sustaining days will be lesser [25][26]. A novel algorithm which takes less processing cycles and memory to make connection secure and should be ideal in IoT conditions is not being addressed [18].

From the analysis of literature, some of the research gaps observed for a lightweight device that needs to be addressed are

a. Data security architecture suitable for a heterogeneous IoT environment to make different IoT devices to share common authentication, authorization, data transaction schemes or protocols [21].

b. Packet level threat detection mechanism in sensor network, to have a trusted scheme, device detection and authorization in network [23].

c. Secure data communication channels which is suitable in a resource constraint IoT environment.

Internet of Things is making way through modern-day lifestyle and strives to improve life's quality by joining us with various smart devices, technologies, and applications. IoT aims to generate a setting where there is complete automation everywhere [27]. Numerous researches have been performed in IoT, but still there is further exploration to be done [24][25]. The upsurge of industries and governments in this field led to a widespread in research and has ensued in numerous successful projects. Some trials in IoT like overall architecture, security and privacy concerns have garnered more attention, while other concerns like availability, reliability, and performance of the smart devices necessitate further investigation. In this paper we have debated the various architectures, security, privacy problems and lightweight solutions used to solve them.

References

1. Chernyshev, Maxim, et al. "Internet of things (iot): Research, simulators, and testbeds." IEEE Internet of Things Journal 5.3 (2017): 1637-1647.

2. Bhardwaj, Isha, Ajay Kumar, and Manu Bansal. "A review on lightweight cryptography algorithms for data security and authentication in IoTs." 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2017.

3. Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." 2017 International Conference on Inventive Systems and Control (ICISC). IEEE, 2017.

4. Kamal, Mohsin. "Light-weight security and data provenance for multi-hop Internet of Things." IEEE Access 6 (2018): 34439-34448.

5. Tsai, Kun-Lin, et al. "AES-128 based secure low power communication for LoRaWAN IoT environments." IEEE Access 6 (2018): 45325-45334.

6. Tao, Hai, et al. "Secured data collection with hardware-based ciphers for IoT-based healthcare." IEEE Internet of Things Journal 6.1 (2018): 410-420.

7. Kim, Young-Sae, and Geonwoo Kim. "A Performance Analysis of Lightweight Cryptography Algorithm for Data Privacy in IoT Devices." 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018.

8. Tedeschi, Pietro, et al. "LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications." IEEE Internet of Things Journal 7.1 (2019): 621-638.

9. U. 42, "2020 Unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report", Unit42, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/. [Accessed: 18- Jul- 2020].

10. NISTIR 8114, report on lightweight cryptography. (n.d.). NIST Computer Security Resource Center CSRC. https://csrc.nist.gov/publications/detail/nistir/8114/final

11. Indira Kalyan Dutta, Bhaskar Ghosh and Magdy Bayoumi, “Lightweight Cryptography for Internet of Insecure Things: A Survey” 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) DOI: 10.1109/CCWC.2019.8666557 7-9 Jan. 2019.

12. Nilupulee A Gunathilake, William J. Buchanan and Rameez Asif, “Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications” 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) DOI:10.1109/WF-IoT.2019.8767250 15-18 April 2019.

13. Sriram Sankaran, S. Shivshankar and K. Nimmy, “LHPUF: Lightweight Hybrid PUF for Enhanced Security in Internet of Things” 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) DOI:10.1109/iSES.2018.00066 17-19 Dec. 2018.

14. Krishna Prasad, Satamraju and B. Malarkodi, “Design and Evaluation of a Lightweight Security Framework for IoT Applications” TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON) DOI:10.1109/TENCON.2019.8929306 17-20 Oct. 2019.

15. Effy Raja Naru, Hemraj Saini and Mukesh Sharma, “A recent review on lightweight cryptography in IoT” 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) DOI:10.1109/I-SMAC.2017.8058307 10-11 Feb. 2017.

16. Vishal Prakash, Ajay Vikram Singh and Sunil Kumar Khatri, “A New Model of Light Weight Hybrid Cryptography for Internet of Things” 2019 3rd International

conference on Electronics, Communication and Aerospace Technology (ICECA) DOI:10.1109/ICECA.2019.8821924 12-14 June 2019.

17. Victor Kathan Sarker, Tuan Nguyen Gia, Hannu Tenhunen and Tomi Westerlund, “Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes” ICC 2020 - 2020 IEEE International Conference on Communications (ICC) DOI:10.1109/ICC40277.2020.9149359 7-11 June 2020.

18. Ravi Raushan Kumar Chaudhary and Kakali Chatterjee, “An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System” 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN) DOI:10.1109/SPIN48934.2020.9071421 27-28 Feb. 2020.

19. T. Goyal, V. Sahula and D. Kumawat, "Energy Efficient Lightweight Cryptography Algorithms for IoT Devices", IETE Journal of Research, pp. 1-14, 2019. Available: https://doi.org/10.1080/03772063.2019.1670103.

20. H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier and M. Mansour, "One round cipher algorithm for multimedia IoT devices", Multimedia Tools and Applications, vol. 77, no. 14, pp. 18383-18413, 2018. Available: https://doi.org/10.1007/s11042-018-5660-y.

21. G. Mustafa, R. Ashraf, M. Mirza, A. Jamil and Muhammad, "A review of data security and cryptographic techniques in IoT based devices", Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS '18, pp. 1-9, 2018. Available: https://doi.org/10.1145/3231053.3231100.

22. M. Schuß, J. Iber, J. Dobaj, C. Kreiner, C. Boano and K. Römer, "IoT Device Security the Hard(ware) way", Proceedings of the 23rd European Conference on Pattern Languages of Programs, pp. 1-4, 2018. Available: https://doi.org/10.1145/3282308.3282329.

23. W. Buchanan, S. Li and R. Asif, "Lightweight cryptography methods", Journal of Cyber Security Technology, vol. 1, no. 3-4, pp. 187-201, 2017. Available: https://doi.org/10.1080/23742917.2017.1384917.

24. D. Mendez Mena, I. Papapanagiotou and B. Yang, "Internet of things: Survey on security", Information Security Journal: A Global Perspective, vol. 27, no. 3, pp. 162-182, 2018. Available: https://doi.org/10.1080/19393555.2018.1458258.

25. R. Fatima, R. Manal and M. Tomader, "Cryptography in e-Health using 5G based IOT", Proceedings of the 4th International Conference on Big Data and Internet of Things, pp. 1-6, 2019. Available: https://doi.org/10.1145/3372938.3372955.

26. Georgiadis, M. Dossis and S. Kontogiannis, "Performance evaluation on IoT devices secure data delivery processes", Proceedings of the 22nd Pan-Hellenic Conference on Informatics - PCI '18, pp. 306-311, 2018. Available: https://doi.org/10.1145/3291533.3291569.

27. Durand, P. Gremaud, J. Pasquier and U. Gerber, "Trusted Lightweight Communication for IoT Systems Using Hardware Security", Proceedings of the 9th

International Conference on the Internet of Things - IoT 2019, pp. 1-4, 2019. Available: https://doi.org/10.1145/3365871.3365876.

28. R. Bali, F. Jaafar and P. Zavarasky, "Lightweight authentication for MQTT to improve the security of IoT communication", Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19, pp. 6-12, 2019. Available: https://doi.org/10.1145/3309074.3309081.

Shreyas S received his M. Tech from in Computer Networks & Engineering from Visveswaraya Technological University. He is currently pursuing the Ph.D. degree in computer science engineering at R.V College of Engineering Bangalore, India. His research areas include cryptography & Network security.

Nagaraja G.S, working as professor, Associate Dean PG-CNE at R.V College of Engineering Bangalore, India. He is a Senior IEEE member. He has authored and co-authored various National & International Journals papers, book chapters, His area of interest include Computer Networks & Management, Multimedia Communications.