International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3854–3862

A Survey on Secured Authentication Schemes over IoT Devices

Krishna Priya Gurumanapalli
Research Scholar, Dept.of Computer Science and Technology
Sri Krishnadevaraya University
Anantapuramu, Andhra Pradesh, India
priya.racharla@yahoo.com

M. Nagendra
Professor, Dept.of Computer Science and Technology
Sri Krishnadevaraya University
Anantapuramu, Andhra Pradesh, India
nagendra_m@rediff.com

Abstract

Internet of Things (IoT) is a network of universal things such as physical objects, machines, people and other devices that enable connectivity and communications to exchange data for intelligent applications and services. The hardware of IoT is susceptible to the security threats from various malicious users. Since, the IoT affected due to the inherent mobility of the embedded devices. The reliability and security of IoT during data transmission is achieved by securing the hardware architecture of the IoT devices. There are two different security mechanisms such as light weight cryptography algorithms and two factor authentication scheme used to secure the IoT. In this paper, the important definition about the internet of things is described with its possible secure mechanisms used to secure the data transmission. This paper evaluates the existing methods that used to secure the IoT with its limitations. The execution time is considered as key parameter for defining the effectiveness of authentication methods used in the IoT. This comprehensive research helps the researchers for achieving the better solution for the current concerns faced in authentication methods in the IoT.

Keywords—*Execution Time, Internet of Things, Light Weight Cryptography, Security Threats, Two Factor Authentication Scheme.*

I. INTRODUCTION

IoT is generally a network of objects, physical devices, vehicles, buildings and other devices which are integrated with sensors, software, electronics and network connectivity. Since, these objects are coupled together to transmit the data among the objects. Additionally, the communication is achieved between the objects and digital devices without any interference of human [1], [2]. There are two types of communication modes achieved in the data transmission among the objects. The types of communication modes are Machine-to-Machine (M2M) and Machine to Cloud (M2C). In M2M mode, the smart object exchange and transmits the data in decentralized manner without using any centralized system. But, in M2C mode the centralized data transmission is achieved among the smart objects and cloud [3]. In addition, the IoT used in different industrial fields such as smart city, smart grid, environment monitoring, e-home, e-health, etc [4]. For example, the patient monitoring quality is improved by using the mobile health care technology. This helps to obtain the faster involvement in critical solutions [5], [6].

In IoT environment, most of the devices are connected through wireless connections and it is operated in un trusted environmental conditions. An unauthorized user maliciously adjusts the hardware infrastructures because of the distributed deployment nature and inherent mobility of the network [7]. The integration of IoT and smart devices are affected because of threats to the privacy and security. Due to the capacity of storing the critical user information, the IoT communication is affected

ISSN: 2233-7857 IJFGCN

to the security threat. The various IoT security issues are illegal access to information, authentication, authorization, privacy, tracking of the data stream, platform management, organization, data integrity, and data confidentiality. In that, a user authentication is considered as an important issue because of the privacy leakage and user security in IoT [8]. Additionally, there are three different challenges are considered while deploying the security solutions such as less overhead, less power consumption and it requires adequate performances for supporting the end user requirements. The conventional methods used for improving the security are Welch-Gong stream cipher [9] and elliptic curve cryptography [10]. This paper delivers the analysis about the various authentication methods used in the IoT. Moreover, this paper specifies the merits and limitations of various authentication methods.

The overall organization of this paper is given as follows: The overview about IoT, description about authentication methods and examples of authentication methods are given in section II. Then the literature survey about the existing techniques are presented in section III. The general security threats found from IoT are mentioned in section IV. Finally, the conclusion is made in section V.

II. OVERVIEW OF AUTHENTICATION IN IOT

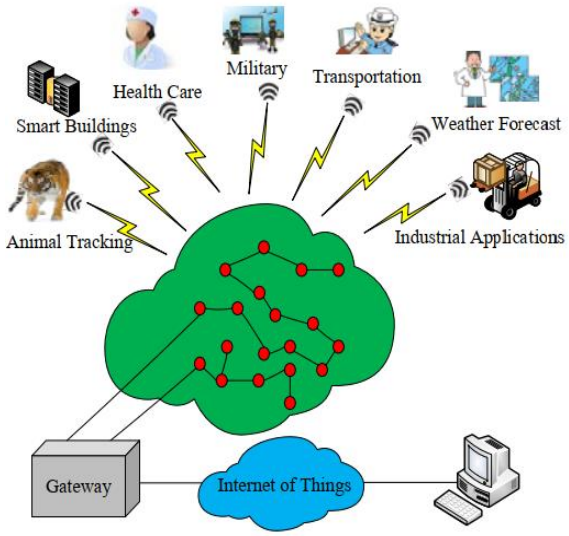

Fig. 1. IOT in various domains

IoT is considered as the initial development of the Internet. IoT is generally a global network which transmits the huge amount of data which is used for intelligent decision making. Nowadays, the IoT plays significant role throughout the world for improving the human's life quality. The general architecture of IoT scenario [11] is illustrated in the Figure 1.

The Internet of Things (IoT) service is vulnerable to various security threats due to the nature of IoT technology. These vulnerabilities are mitigated by using different authentication mechanisms such as light weight cryptography and two factor authentication.

A. Lightweight cryptography

Lightweight cryptography is one of the security systems which are designed for restricted devices. The main concentration in the lightweight algorithm design is hardware implementation. The logic gate which is required for operating the various programs is specified as Gate Equivalent (GE). The algorithm is referred as lightweight, when it utilizes the less amount of GE. The main reasons to use the light weight cryptography are given as follows:

1) Efficiency of end-to-end communication

The symmetric key algorithm is used in the nodes of IoT network for achieving the end-to-end security. In cryptographic operation, the less energy consumption is considered as important during the data transmission in IoT. Therefore, battery powered devices are utilized for the low resource-devices.

ISSN: 2233-7857 IJFGCN

Then the lesser energy consumption for the digital devices are achieved by using the applications of light weight key algorithm.

2) Applicability to lower resource devices

The complexity of the lightweight cryptographic algorithm is lesser than the conventional cryptography algorithm. The lightweight cryptographic algorithm is operated with lower resource devices.

B. Two factor authentication

The strong authentication and controlling access to the resources and network are considered as essential security requirements for the IoT. The three factors mainly utilized for authentication are biometrics, tokens and passwords. Here, the combination of two factors namely two factor authentication are frequently used for improving the security of authentication. Since, the IoT devices are operated without any human interference. Therefore, the password is stored in the memory for enabling the authentication. But the tokens used for the authentications are not considered as an adequate for wireless communications.

C. Examples of authentication schemes

In this section, the examples of authentication schemes used in the IoT are described with its process.

1) Label based authentication protocol

The caching fog node's status are authenticated by using the Caching Server (CS). This authentication is done by checking the values of data embedded label. Additionally, this CS evaluates whether the fog node connects with the caching services or not. Since, the evaluation process is done based on the authentication's outcome. The steps processed in the label based authentication protocol [12] are given as follows:

a. Initially, the *encode* function is used by the CS for creating the file handle η as the unique symbol. This $encode$ function converts the file $\tilde{F}$ into $\tilde{F}_\eta$. Where, the function encode is represented as $(\tilde{F}; k)[\pi] \rightarrow (\tilde{F}, \eta)$.

b. The output value c of the $challenge$ function is used by CS for file $\tilde{F}_\eta$, where the $challenge$ function is $(\eta, k)[\pi] \rightarrow c$.

c. For each challenge value of c, the fog node utilizes the *respond* function for creating the Γ. where $(c, \eta) \rightarrow r$ represents the *respond* function.

d. The *verify* function is used by the CS for detecting whether r specifies an adequate response to the challenge value c. If the verification succeeded, this function delivers the output as Boolean variable '1'. The verify function is represented as $((r, \eta); k) \rightarrow b \in \{0,1\}$.

2) Lightweight and privacy-preserving two-factor authentication

In this lightweight and privacy-preserving two-factor authentication [13], the security is developed by using four different phases such as request for interaction, server response, server authentication and device authentication.

a) Request for interaction

At first, one time alias identity is selected, when the IoT device is interacted with the server. Then the random number N_d is generated and it calculates the N_b^*. Here, the device has a request message which is transmitted to the server for interaction purpose.

b) Response from server

The one-time alias identity is located by the server, when the authentication request message is received in the server. Then this alias identity is read and loaded into the memory. After that, the server

ISSN: 2233-7857 IJFGCN

creates the nonce N_s and identifies the, N_s^* key hash response as well as it contains response message which is transmitted to the device.

c) Server authentication

The output of PUF is extracted while receiving the response message. Then the key hash response is calculated and checked like whether it is valid or not. The protocol execution is terminated by the device, when the key hash response is not valid. Otherwise, the server is going to be authenticated and decodes the N_s. Then the key element and helper data are obtained from the helper data generation algorithm. Then the message from the device should transmit to the server.

d) Device authentication

The server calculates and decodes the helper data while receiving the message. The key element is obtained using the reconstruction algorithm. Then the key hash response is verified by server. The session key is calculated and device is authenticated, when the verification is successful. Then the server calculates new challenge and decodes new PUF output as well as it updates the alias identity. Additionally, the alias identity is stored in the server for next interaction with the device.

The server uses the unused pairs to perform try again operation, when the server doesn't identify the IoT device at step 2. The used pairs are eliminated in both the ends. In that case, the server selects one of the unutilized CRP and new alias identity. The used CRP also deleted in this two factor scheme. This helps to control the de-synchronization problem without negotiating the privacy.

III. LITERATURE SURVEY

In the development of secured IoT, various researches are developed by researchers. This section gives the brief evaluations of some important contributions to the existing literatures which are given as follows:

Li, W., Liao, L., Gu, D., Li, C., Ge, C., Guo, Z., Liu, Y. and Liu, Z [11] presented the LED cipher by developing the Ciphertext-only Fault Analysis (CFA) with 6 different distinguishers. The 6 distinguishers considered in the CFA are Square Euclidean Imbalance (SEI), goodness of fit (GF), GF-SEI, maximum likelihood, Hamming weight, and maximum a posteriori distinguisher. The performance analyzed in this CFA are latency and time complexity. The integration of CFA with 6 various distinguishers are used to minimize the amount of faults and enhance the attacking efficiency. But, the time complexity of the LED-128 is high for SEI than the remaining distinguisher.

Wang, Q., Chen, D., Zhang, N., Qin, Z. and Qin, Z. [12] developed the lightweight label-based access control scheme (LACS) for preserving the catching from the security concerns. This LACS authenticates the fog nodes in the IoT for ensuring the protection. Since, the authentication process is carried out by validating the transmitted file's integrity. The performance analyzed by the LACS are blocks permuting delay, file partitioning delay, label embedding delay, label generating delay, probability of adversary detection and verification delay. The developed LACS achieves the milliseconds based verification. However, the overhead of this LACS based IoT got increased with the increment in block size.

Bansod, G., Patil, A., Sutar, S. and Pisharoty, N [14] presented the ultra-lightweight cipher ANU to secure the IoT. ANU is generally a balanced feistel-based network. Additionally, this ANU supports the plaintext of 64 bit, key length of 128/80 bit and this ANU totally has 25 rounds. The performances analyzed for the ultra-lightweight cipher are the computation of Gate Equivalent (GE), memory requirement and power consumption. The developed ANU requires only 1015 gate equivalents for 128 bit key length which is less when compared to the existing lightweight ciphers. The computational complexity during the biclique attack comparison is high.

Lara-Nino, C.A., Diaz-Perez, A. and Morales-Sandoval, M [15] developed the hardware implementations of PRESENT for mitigating the security concerns under extremely constrained environments. There are five different architectures of PRESENT are analysed in IoT such as Iterative (C1), Serial (C2), 16-Bit (C3), 16-Bit With 80-Bit Keys (C4) and 16-Bit With 128-Bit Keys (C5). The performances evaluated for PRESENT architecture are area, circuit count, energy, flip flops, key size,

ISSN: 2233-7857 IJFGCN

latency, look-up tables, operational frequency, power, throughput and slices. The designs of C4 and C5 has less area and less energy consumption than the other designs. The throughput for the developed architecture C4 and C5 are less when compared to the remaining architecture.

Alassaf, N., Gutub, A., Parah, S.A. and Al Ghamdi, M. [16] presented a light weight cryptographic algorithm based on the SIMON for health care applications. The developed SIMON is analyzed for different block sizes such as 32, 48, 64 and 96 bits. The evaluated performances of for a light weight cryptographic algorithm are execution time and memory occupancy. This improved SIMON minimizes the encryption time and it maintains the balance among the performances and security. The ROM memory occupancy of the optimized SIMON is high when compared to the conventional SIMON.

Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R. and Mansour, M.M. [17] used the dynamic structure with single round for developing the lightweight cipher algorithm which has only simple operations. This cipher algorithm is concentrates on the multimedia IoT. In dynamic structure, the dynamic key is generated for different multimedia contents like image/video or audio. The evaluated performances of lightweight cipher algorithm are execution time, Peak Signal-To Noise Ratio (PSNR), and Structural Similarity Index (SSIM). The amount of rounds is reduced into a single one by using this dynamic cipher structure. But, the amount of memory occupied during the authentication is not evaluated in this work.

Guo, X., Hua, J., Zhang, Y. and Wang, D. [18] developed the secure and fast encryption routine (SAFER) as fermat block encryption method in IoT. In SAFER-Fermat encryption algorithm, the diffusion layer is built by using the fast Fermat number theory transform (FNTT). The performance analyzed for SAFER-Fermat encryption are PSNR and SSIM. This SAFER-Fermat algorithm provides the security in lesser cost and it has less computational complexity. The performances of the SAFER-Fermat encryption algorithm is less for some images when compared to the conventional SAFER algorithm.

Biswas, A., Majumdar, A., Nath, S., Dutta, A. and Baishnab, K.L [19] presented the lightweight encryption method namely LRBC is developed for resource constraint IoT devices that delivers data security in the sensing level. Additionally, an encryption approach is used for accompanying the round key management strategy. The performances evaluated for the LRBC are area, avalanche effect, hamming distance and maximum frequency. In IoT, the security is improved by using the advantages of Feistel structure and substitution–permutation network in LRBC. Here, the efficiency is analyzed only based on the avalanche effect, but it fails to analyze the execution time.

Patil, A., Bansod, G. and Pisharoty, N. [20] developed a robust hybrid structure in IoT by fusing the LED, SPECK and RECTANGLE. The clustering of differential and linear trails is eliminated by utilizing the bit slicing method and S-box of the RECTANGLE. The evaluated performances of robust hybrid structure are execution time, flash memory, GE, number of cycles, RAM memory and throughput. Here, the LED's key scheduling aspects is enhanced and crucial attacks are mitigated in LED cipher by using this hybrid design. The execution time of this hybrid structure is high, when compared to the conventional structures.

Aman, M.N., Basheer, M.H. and Sikdar, B [21] presented the location based authentication protocol for securing the IoTsystems. The hardware authentication, creating a trust root and secure key generation are achieved by integrating the Physically Unclonable Functions (PUFs) in the authentication protocol. Additionally, this location based authentication utilizes the IoT node’s location in the circular area as 2nd factor for authentication. The evaluated performances of the authentication protocol are average received power, probability of detection, communication overhead and radio transceiver energy. This location based authentication protocol achieves lesser energy consumption and it has less computational complexity. But, the detection probability is minimized, when the node moved towards the center point of the network.

Karthigaiveni, M. and Indrani, B [22] developed the password based authentication scheme by integrating the Elliptic Curve Cryptography (ECC) and smart card. This scheme is generally a two factor authentication scheme that is integrated with password and smartcard. The performances analyzed for the password based authentication scheme are communication cost, execution time and

ISSN: 2233-7857 IJFGCN

total cost. The usages of ECC for creating the session key improves the security of the IoT. Since, this session key is utilized for mutual authentication symmetric key cryptography. But, the ECC used in the encryption scheme generally increases the size of the encrypted message.

Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P. [23] presented the Lightweight Scalable Blockchain (LSB) to provide the end-to-end security and this LSB is optimized based on the requirements of IoT. Here, a Distributed Time-based Consensus algorithm (DTC) is developed for minimizing the delay and mining processing overhead. The performances analyzed for the LSB is processing time. The processing overhead to verify the new blocks are reduced by using the distributed trust approach in IoT. Moreover, the distributed trust algorithm employed by the LSB analyses only less amount of transactions.

Li, X., Niu, J., Bhuiyan, M.Z.A., Wu, F., Karuppiah, M. and Kumari, S [24] developed the security in the Industrial Internet of Things (IIoT) by developing the user authentication protocol scheme. This proposed scheme is analyzed in random oracle model and the analyzed performances of user authentication protocol are end to end delay, packet delivery ratio and throughput. This authentication protocol avoids the common attacks with less computational efficiency. But, the throughput over the IoT scheme is increased while increasing the sensor nodes over the network. Meanwhile the congestion also increases with respect to the increment in sensors.

Lohachab, A [25] presented the Message Queuing Telemetry Transport (MQTT) and ECC for creating the light-weight authentication and authorization framework in distributed IoT environment. The MQTT is used to obtain the broadcast based data transmission and the evaluated performances of MQTT are attack search time, computational cost and execution time. The ECC used to improve the security with smaller size of key. But, the implementation of ECC is difficult.

Gope, P. and Sikdar, B [13] developed a lightweight and privacy-preserving two-factor authentication for addressing the issues of IoT devices. Here, the PUFs are considered as one of the authentication factor. Additionally, the reverse fuzzy extractor is used for eliminating the issue occurred because of the noise during the operation of PUF. The performances analyzed for this two-factor authentication schemes are computational cost, execution time and security features. An essential feature of PUF are used in the authentication scheme to provide the adequate security characteristics for IoT. This two factor algorithm provided the security only at the physical layer.

IV. CHALLENGES AND RESEARCH SOLUTION

The integration of the IoT with the different object creates the various issues in people's daily life. Therefore, delivering the robust security to the IoT is considered as challenging during the transmission.

The major problems and the possible attacks faced by the IoT are specified as follows:

Node capture: Nodes (i.e., gateway or base node) are controlled by the attackers. The protocol states and cryptographic keys are obtained by controlling the nodes with attackers. Additionally, this node capture duplicates and distributes the malicious nodes over the network which degrades the IoT performances.

Routing Threats: The routing threat over the IoT is considered as important attack which happened in perception layer of IoT. Here, the attacker generates the routing loop that causes the higher error messages, extension/ shortage in routing path and higher end to end delay.

Physical attacks: Generally, the physical attacks are focused on the hardware devices of the system.

Impersonation attack: The malicious attacker is act like authenticate server/user by providing the reply to the valid request message from the earlier communication among two authenticate devices. In that case, a malicious attacker obtains similar authorization and service as an authenticate user or server.

ISSN: 2233-7857 IJFGCN

Message tampering attack: The message tampering attack creates the issues in the message integrity. In general, the nodes in the network listen all the data's transmitted by the remaining nodes. In that case, the malicious node may change the contents of the data before transmitting to the desired user.

Replay Attack: In replay attack, the data is stored and retransmitted without using any authority. Such attacks are commonly used against authentication protocols.

Brute-force attack: Generally, brute-force attack is referred as password guessing attack. The brute-force attack is an attempt for identifying the password by analytically trying every possible combination of letters, numbers, and symbols.

Especially in the two factor algorithm which considers the PUF [13] was used to deliver the robustness to the security. This light weight and privacy preserving two factor algorithm was provided the security only at the physical layer. But it requires one more cryptography algorithm for achieving the data security. The distinctive feature of the PUF is that it generates identical code for the all devices in the system. This PUF can be identified by using the developed Artificial intelligence(AI), machine learning techniques.

Research solution:

As mentioned in the previous section, the PUF circuit can generate a different function for different devices but it is fixed for each device. All the IoT devices are equipped with a PUF, where any attempt to tamper with the PUF will change the behavior of the device and render the PUF useless. To overcome this problem, a dynamic path reconfiguration model is introduced in PUF with adaptive circuit transformation mechanism on the basis of device behavior. By introducing this approach in existing system TFA scheme, the device can generate different unclonable function for each interaction between server and device. For each interaction, the physical path between logic gates or circuit of PUF-IC can modify itself to generate CRP unpredictable challenge-response behavior. To ensure data security, the CRP scheme with binary shift and complement algorithm will apply to data to ensure high differentiation between data and CRP.

V. CONCLUSION

The IoT faces various challenges and issues such as memory space, performance cost, device's power consumption, restricted memory capacity and security threats. In that, security is considered as a main concern due to the data leakage and access of unauthorized users while transmitting the data. This paper provides the overview about the IoT and also it specifies types of authentication methods used in the IoT. The various authentication techniques are also analyzed with its merits, demerits and performance measure. This research is very helpful in finding the authentication methods current trends and next level of problem identification. Still, there is much work to be done on the authentication methods over IoT. This research paper will help the readers to understand the state-of-the-art in the process of authentication methods used in the IoT and also motivate more meaningful works.

REFERENCES

[1] P. K. Panda, and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," Journal of Reliable Intelligent Environments, pp.1-16, 2020.

[2] M. Wazid, A. K. Das, S. Shetty, "JPC Rodrigues, J. and Park, Y., 2019. LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment," Sensors, vol. 19, pp.5539, 2020.

[3] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron, "New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications," Peer-to-Peer Networking and Applications, vol. 13, pp.439-474, 2020.

ISSN: 2233-7857 IJFGCN

[4] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Future Generation Computer Systems, vol. 49, pp.104-112, 2015.

[5] S. Roy,S. Chatterjee, A. K. Das,S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things," IEEE Internet of Things Journal, vol. 5, pp.2884-2895, 2017.

[6] S. D. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in IoT-based healthcare environment," Journal of Reliable Intelligent Environments, pp.1-11, 2019.

[7] Z. Huang, and Q. Wang, "A PUF-based unified identity verification framework for secure IoT hardware via device authentication," World Wide Web, pp.1-32, 2019.

[8] B. H. Taher, S. Jiang,A. A. Yassin, and H. Lu, "Low-Overhead Remote User Authentication Protocol for IoT Based on a Fuzzy Extractor and Feature Extraction," IEEE Access, vol. 7, pp.148950-148966, 2019.

[9] X. Fan,K. Mandal, and G. Gong, "Wg-8: A lightweight stream cipher for resource-constrained smart devices," In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness,Springer, pp. 617-632, 2013.

[10] A. K. Das, M. Wazid,A. R. Yannam,J. J. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment", IEEE Access, vol. 7, pp.55382-55397, 2019.

[11] W. Li, L. Liao, D. Gu, C. Li, C. Ge, Z. Guo, Y. Liu, and Z. Liu, "Ciphertext-only fault analysis on the led lightweight cryptosystem in the internet of things," IEEE Transactions on Dependable and Secure Computing, vol. 16, pp.454-461, 2018.

[12] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context," IEEE Access, vol. 5, pp.4018-4027, 2017.

[13] P. Gope, and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices", IEEE Internet of Things Journal, vol. 6, pp.580-589, , 2018.

[14] G. Bansod, A. Patil,S. Sutar, and N. Pisharoty, "ANU: an ultra lightweight cipher design for security in IoT," Security and Communication Networks, vol. 9, pp.5238-5251, 2016.

[15] C.A. Lara-Nino,A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight hardware architectures for the present cipher in FPGA," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 64, pp.2544-2555, 2017.

[16] N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi,"Enhancing speed of SIMON: a light-weight-cryptographic algorithm for IoT applications", Multimedia Tools and Applications, vol. 78, pp.32633-32657, 2019.

[17] H. Noura, A. Chehab,L. Sleem, M. Noura, R. Couturier, and M.M. Mansour, "One round cipher algorithm for multimedia IoT devices," Multimedia tools and applications, vol. 77, pp.18383-18413, 2018.

[18] X. Guo, J. Hua, Y. Zhang, and D. Wang, "A Complexity-Reduced Block Encryption Algorithm Suitable for Internet of Things", IEEE Access, vol. 7, pp.54760-54769, 2019.

[19] A. Biswas,A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab, "LRBC: a lightweight block cipher design for resource constrained IoT devices," Journal of Ambient Intelligence and Humanized Computing, pp.1-15, 2020.

[20] A. Patil, G. Bansod, and N. Pisharoty, "Hybrid lightweight and robust encryption design for security in IoT," International Journal of Security and Its Applications, vol. 9, pp.85-98, 2015.

[21] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for IoT with location information," IEEE Internet of Things Journal, vol. 6, pp.3335-3351, 2018.

[22] M. Karthigaiveni, and B. Indrani, "An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card," Journal of Ambient Intelligence and Humanized Computing, pp.1-12, 2019.

ISSN: 2233-7857 IJFGCN

[23] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," Journal of Parallel and Distributed Computing, vol. 134, pp.180-197, 2019.

[24] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, pp.3599-3609, 2017.

[25] A. Lohachab, "ECC based inter-device authentication and authorization scheme using MQTT for IoT networks,"Journal of Information Security and Applications, vol. 46, pp.1-12, 2019.

ISSN: 2233-7857 IJFGCN