A review on data Security, Security Threats and Solution in IoT Environment

[1]MANISH KUMAR TWINKLE, [2]SHITAL GUPTA

SCHOOL OF RESEARCH AND TECHNOLOY, PEOPLE'S UNIVERSITY, BHOPAL

Abstract- Internet of Things may be a network of universal things like physical objects, machines, people and other devices that enable connectivity and communications to exchange data for intelligent applications and services. IoT request domains are very huge including smart cities, smart homes, e-health, wearable, etc. Billions of devices will be associated in IoT communications. Such devices will have smart capabilities to gather , analyze and even make decisions with none human interaction. Security may be a supreme requirement in such circumstances and especially authentication is of high interest given the damage that would happen from a malicious unauthenticated device in an IoT system. This paper evaluates the existing methods that used to secure the IoT Infrastructure. This paper gives complete and up-to-date view of the IoT authentication field. It provides a summary of an outsized range of authentication protocols. The study will helps the researchers for achieving the better solution for the current concerns faced in authentication methods in the IoT Infrastructure.

Keywords: Internet of Things, Cryptography, Encryption, Security Threats, confidentiality, Authentication.

1.1 INTRODUCTION

Internet of Things is a great network of networks involving smart devices such as sensors and actuator. These devices are adopted in a variety of domains such as community health, smart grids, smart shipping, waste management, smart homes, smart cities, and agriculture and energy organization. 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. 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). But, in M2C method the centralized data communication is achieved between the smart objects and cloud [3]. In IoT environment, most of the devices are connected through wireless connections and it is operated in untrusted environmental conditions. An unconstitutional user maliciously adjusts the hardware infrastructures since of the dispersed deployment character and inherent mobility of the network [4]. 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 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. User authentication is considered as an important issue because of the privacy leakage and user security in IoT[5]. 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 specific scenery of IoT devices makes the conventional authentication schemes infeasible and not appropriate. Indeed, cryptographic schemes designed for security require high processing and large memory. This led to the appearance of unimportant validation schemes. The security requirements of an IoT network mainly depend on the type of applications it serves, the need for confidentiality, integrity and authentication directly depends on the security needs of the application. In particular, authentication is considered as a key requirement for IoT.

1.2 RELEATED WORK

Biswas, A., Maunder et. al [6] 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. Karthigaiveni, M. et. al [7] 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 total cost. The usages of ECC for creating the session key improve 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 et. al [8] 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. Alassaf, N., Gutub et. al [9] 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.Guo, X., Hua et. al [10] 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 is 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. Lohachab, A et. al [11] 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. Li, W., Liao et. al [12] presented the LED cipher by developing the Cipher text-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. Noura, H., Chehab et. al [13] 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. Aman, M.N., Basheer et. al [14] presented the location based authentication protocol for securing the IoT systems. The hardware authentication, creating a trust root and secure key generation are achieved by integrating the Physically Uncountable 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. Gope, P. and Sikdar, B [15] 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. Atwady et. al [16] presented a survey of the authentication protocols deployed in Internet of Things (IoT) use cases by categorizing them into four categories: Internet of Sensors (IoS), Internet of Energy (IoE), Machine-to-Machine (M2M) communication, and Internet of Vehicles (IoV). A taxonomy and comparison of authentication protocols are provided in terms of: network model, goals, main processes, computation complexity, and communication overhead. E Silva et. al [17], mapped the current state of the art of the authentication in an IoT environment, featuring the difficulties and the primary methods utilized in authentication scheme but without performing any comparison. Gebrie, M.T et. al [18] provided a brief overview of authentication mechanisms with an evaluation of the proposed schemes in the literature. They also evaluated each method based on its resource consumption (e.g., energy, memory computation and communication)

1.3 IOT GENERIC ARCHITECTURE

Even as ancient web connects community to a network, IoT incorporates a dissimilar approach within which it affords Machine-to-Machine (M2M) and Human-to-Machine (H2M) property for numerous varieties of machines in organizes to support diversity of applications. The essential design model projected within the literature is three-layer design.

Perception layer: physical layer that senses the environment to understand the physical assets (e.g. humidity, temperature, speed, location, etc.) exploitation end-nodes through the utilization of various sensing technologies (e.g., RFID, GPS, NFC, etc.). Network Layer: it's the layer guilty of obtaining knowledge from the perception layer and transmittal it to the applying layer through numerous network technologies (e.g., 3G, 4G, 5G, Wi-Fi, Bluetooth, Zig-Bee, etc.). This is often additionally dependable of knowledge managing from storing to process with the assist of middle-wares like cloud computing. Application Layer: the layer that's in accuse of delivering application-specific services to the consumer. The importance of this layer is that it's the power to hide various markets (e.g., good cities, good homes, health care, building automation, good metering, etc.

1.4. SECURITY ISSUES IN IOT:

The main IoT security considerations are:

Authentication: the method the method and insuring the identity of objects. In IoT context every object ought to have the flexibility to spot and manifest all alternative objects within the system.

The authorization: the method of giving permission to AN entity to try and do one thing [19].

Integrity: the method of maintaining the consistency, exactitude and irresponsibleness of knowledge over its whole life cycle. In IoT, the alteration of basic data or maybe the infusion of invalid data might prompt major problems, e.g., in sensible health systems use cases it could lead on to the death of the patient.

Confidentiality: the method of guaranteeing that the knowledge is barely accessed by approved individuals. 2 main problems ought to be thought-about concerning in IoT: first to make sure that the thing receiving knowledge the information} isn't getting to move or transfer these data to alternative objects and second to contemplate the information management.

Non-repudiation: The manner toward guaranteeing the flexibility to demonstrate that a task or event has occurred with the goal that this cannot be denied later.

Availability: the method of guaranteeing that the service required is out there anyplace and anytime for the meant users. This includes in IoT, the supply of the objects themselves.

Privacy: the method of guaranteeing non-accessibility to non-public data by public or malicious objects.

1.5 SECURITY CHALLENGES IN IOT LAYERS:

1.5.1. Perception Layer Security problems and Recommendation.

The perception layer consists of sensors that square measure characterized by restricted process power and storage capability. Many security problems and attack risks rise thanks to such limitations. Many attacks on the perception layer square measure noticed.

Node Capture: Nodes will be simply controlled by the attackers. Catching a node empowers AN human not solely to induce tightly of scientific discipline keys and protocol states, however additionally to clone and distribute malicious nodes within the network, that affects the safety of the complete network

Denial of Service (DoS) Attack: a sort of attacks that shuts down the network and prevents approved users from accessing it. This might be achieved by overwhelming the system or network with great deal of spam requests all at a similar time, so overloading the system and preventing it from delivering the traditional service [20].

Denial of Sleep Attack: one amongst the essential objective of an IoT network is that the capability of sensing through an intensive variety of distributed nodes providing tiny knowledge like temperature, humidity, vibration, etc., at a group interval then attending to sleep for one more quantity so as to permit the nodes to control for long service life. The denial of sleep attack works on the ability provide of the node with a significant goal to extend the ability consumption so as to scale back the service life of the node by preventing the node from going asleep when causing the acceptable perceived knowledge.

Distributed Denial of Service (DDoS) Attack: This a another reasonably DoS attacks. The foremost difficult issue is that the ability to use the big quantity of IoT nodes to pass traffic collected toward the victim server.

Fake Node/Sybil Attack: a sort of attacks wherever the wrongdoer will deploy pretend identities victimization pretends nodes. With the presence of a Sybil node, the entire system may generate wrong knowledge or maybe the neighbor nodes can receive spam knowledge and can lose their privacy. The pretend nodes might be wont to transmit knowledge to legitimate nodes leading them to consume their energy that could lead on the entire service to travel down.

Replay Attack: during this attack, data is hold on and re-transmitted later while not having the authority to try and do that. Such attacks square measure unremarkably used against authentication protocols [21][22].

Routing Threats: this sort of attacks is that the most basic attack at the network layer however it may occur at the perception layer in knowledge forwarding method. AN wrongdoer will produce a routing loop inflicting the shortage or extension of the routing path, increasing the end-to-end delay and increasing the error messages.

Side-Channel Attack: this sort of attacks happens on cryptography devices by taking advantage of the hardware data wherever the crypto-system is applied on chips, like the execution time, power consumption, power dissipation, and magnetic force interference made by electronic devices throughout the cryptography procedure. Such data might be analyzed to get secret keys used throughout the cryptography method [23].

Mass Node Authentication: the method of authenticating great deal of devices in an IoT system, which needs large quantity of network communication for the authentication section to finish and this, might have an effect on the performance of the entire system. Taking into thought the preceding risks, there's a desire for node authentication to stop pretend node and bootleg access, additionally to the requirement for encoding to safeguard to safeguard of information whereas being transmitted between nodes. The properties of the nodes with relation to the shortage of power and also the restricted storage capability, there's a necessity for mature light-weight security schemes that embrace each light-weight scientific discipline algorithms and security protocols.

1.5.2. Network Layer Security problems and Recommendation

The network layer is accountable of the diffusion of information from the perception layer to the applying layer. This can be wherever knowledge routing yet because the primary knowledge analysis happens. During this layer many network technologies square measure used like the various technologies for mobile communication generations and wireless networks. Many attacks and risks on the network layer square measure square measure.

Man-in-the-Middle (MITM): The most repeated attacks square measure Denial of Service (DoS) and Man within the Browser (MITB) attacks. This latter, at the side of the Secure Socket Layer (SSL) attack, that allows attackers to pay attention to pay attention, intercept it, and spoof each ends of the information, represent the MITM attack [24].

Denial of Service (DoS): this sort of attacks happens at the network layer by electronic countermeasures the transmission of radio signals, employing a pretend node, touching the transmission or routing of information between nodes.

Eavesdropping/sniffing: this sort of passive attacks offers the persona non grata the flexibility to pay attention to the personal communication over the communication link. The persona non grata could be able to extract helpful data like usernames and passwords, node identification that could lead on to different styles of attacks, e.g., fake node, replay attack etc.

Routing attacks: this kind of attacks affects however the messages or knowledge area unit routed. The persona non grata spoofs, redirects, misdirects or perhaps drops packets at the network layer.

These potential attacks at the network layer result in result in of the subsequent security requirements: hop-to-hop secret writing, point-to-point authentication, key agreement and management, security routing and intrusion detection.

1.5.3 Application Layer Security problems and needs

The application layer is accountable for providing services. It hosts a collection of protocols for message passing [25], e.g., unnatural Application Protocol (COAP), Message Queuing measurement Transport (MQTT), extensile electronic communication and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), etc. This layer directly interacts with the user. Many security problems arise at the applying layer.

Data Accessibility and Authentication: every application might need several users. Artificial or illegal users may have an excellent impact on the provision of the total system. Such nice range of users means that completely different permission and access management.

Data privacy and identity: the actual fact that IoT connects {different| totally completely different| completely different} devices from different makers ends up in the applying of various authentication schemes. the mixing of those schemes could be a difficult issue to confirm knowledge privacy and identity.

Dealing with the provision of huge data: IoT connects an enormous range of finish devices that ends up in an enormous quantity of information to be managed. This causes Associate in nursing overhead on the applying to research this knowledge that contains a huge impact on the provision of the services provided by the applying.

Regarding the safety needs for the applying layer, authentication is needed whereas protective the privacy of users. Additionally there ought to be Associate in nursing data security management theme that features resource management and physical security data management.

1.6 DISCUSSION AND CONCLUSION

In recent years cloud-integrated IoT applications became fashionable among researchers due to their important applications in several organizations. IoT security is Associate in nursing active analysis topic in analysis trade and domain. It desires any attention and study to explore completely different security issues in IoT. This paper investigates major security issues at completely different layers of Associate in Nursing IoT application. The paper conjointly presents the literature review on security in IoT. Numerous open problems and problems that originate from the answer itself have conjointly been mentioned. The Paper gift transient counter measures to completely different security challenges to secure IoT systems. The progressive of IoT security has conjointly been mentioned with a number of the long run analysis directions to reinforce the safety levels in IoT. The future analysis ought to address the problem of security and privacy in IoT environments. This comprehensive study can guide the man of science on wherever efforts ought to be invested with to develop security solutions for IoT.

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

[4] 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.

[5] 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.

[6]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.

[7] 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.

[8] 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

[9] 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

[10] 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.

[11] 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.

[12] W. Li, L. Liao, D. Gu, C. Li, C. Ge, Z. Guo, Y. Liu, and Z. Liu, "Cipher text-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.

[13] 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.

[14] 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.

[15] 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.

[16] Atwady, Y.; Hammoudeh, M. A survey on authentication techniques for the Internet of things. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017;

[17] E Silva, E.d.O.; de Lima, W.T.S.; Ferraz, F.S.; F.I. Authentication and the Internet of Things: A Survey Based on a Systematic Mapping. In Proceedings of the Twelfth International Conference on Software Engineering Advances, Athens, Greece, 8–12 October 2017.

[18] Gebrie, M.T.; Abie, H. Risk-based adaptive authentication for Internet of things in smart home e-Health. In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, Canterbury, UK, 11–15 September 2017; pp. 102–108.

[19] Jung, S.W.; Jung, S. Personal O-Auth authorization server and push OAuth for Internet of Things. Int. J. Distrib. Sens. Netw. 2017.

[20] Anirudh, M.; Thileeban, S.A.; Nallathambi, D.J. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017

[21] Na, S.; Hwang, D.; Shin, W.; Kim, K.H. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017

[22] Tomasin, S.; Zulian, S.; Vangelista, L. Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), San Francisco, CA, USA, 19–22 March 2017.

[23] Shahverdi, A.; Taha, M.; Eisenbarth, T. Lightweight Side Channel Resistance: Threshold Implementations of S imon. IEEE Trans. Comput. 2017, 66, 661–671.

[24] Cekerevac, Z.; Dvorak, Z.; Prigoda, L.; ˇCekerevac, P. Man in the Middle Attacks and the Internet of Things—Security and economic risks. FBIM Trans. 2017, 5, 25–35

[25] Hedi, I.; Speh, I.; Sarabok, A. IoT network protocols comparison for the purpose of IoT constrained networks. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017