Open Research Problem for effective IoT Authentication

Mihir Mehta[1], Kajal Patel[2]
[1]mihir240491@gmail.com, [2]kspldce@gmail.com
[1]Research Scholar, Gujarat Technological University, India,
[2]Associate Professor, VGEC – Chandkheda, India

Abstract
IoT is collection of different "things" which are associated with open web. As all the things are connected to the Internet, it offers convenience to end users for accessing the resources from "Any Where, Any Time" throughout the globe. At the same time, open nature of IoT provides a fertile ground to an intruder for launching different security related threats. If we can no apply proper security safeguards to the IoT System, then it will be not useful to society. Authentication, Encryption, Trust Management and Secure Routing are different domains to offer security in IoT system. Among them, Authentication is very much important security service as it validates device identity before granting access to system services/ resources. Existing IoT Authentication algorithms are fail to verify device identity in unambiguous way. They are vulnerable to different security threats such as Key Stolen threat, MITM threat and Location Spoofing threat. So, it is a demand of time to design an efficient and secure Multi-factor IoT algorithm which can offer better security and validate device identity in unambiguous way.

Keywords:
IOT, Multi-factor Authentication, Context based Authentication, Location Spoofing attack

1. Introduction

Currently, around 20 billion devices are connected to the Internet [1]. As these huge amount of devices are associated with net, it also raises a question for IoT Security [1, 2]. IoT is offering services in different domains such as- Smart City, Smart Health care, Smart Agriculture, Smart Transportation [4]. At the same time, if we do not focus on IoT Security, then there will be no any kind of benefit of these Smart Applications to our Society. All these small gadgets are connected to open web; so, it also opens a door for intruder to perform destructive activities in the IoT network.

One of the major security requirement for IoT Security is Authentication. It validates the identity of device before granting access to the System resources. By implementing strong IoT Authentication, device identity can be verified easily and any illegal attempt for accessing system resources from an intruder can be identified at early stage. Also, strongest IoT Authentication offers security from different security threat such as Key stolen attack, Monitoring attack, Man in the Middle attack and Location Spoofing attack. Apart from Authentication- Encryption, Trust Management and Secure Routing are also other domains in IoT Security. Encryption provides security service in which apart from sender & receiver, no any third party can get access of the data exchange content. Means, data will be exchanged into unreadable form. Trust Management requires to compute trust score dynamically over a period of time for each entity before allowing them into data exchange process. Secure Routing focuses on identifying malicious entity from the network and remove them from the data forwarding process. Among all these Security service, Authentication is prime service for security. Authentication validates identity of device and if it is validated then only device will become part of network for further data exchange process. While other security services focus on security while data are travelling, they do not focus on identity of device or place- origin of data. So, if identity is tampered then there is no meaning of security in the network.

TABLE I: Security Threat for IoT Authentication [6, 7, 8]

Key Stolen Threat	Intruder will get access of key value/ password from device memory or at the time of exchanging handshaking messages between node and server.
Monitoring Threat	Intruder will analyze and capture the traffic passing among various IoT Devices and also between device & Server.
MITM Threat	Intruder will put itself between sender IoT device and receiver IoT device. Intruder will capture all traffic and misuse captured information to launch further attacks on IoT system.
Physical attack	Intruder will get access of IoT device and can make a copy of it's, also can do a mimic of location information of a device to launch attack.

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.19

2. EXISTING APPROACHES FOR IoT AUTHENTICATION

Any of authentication approach from state of art can be categorized into following form:
(1)Identity based authentication [15]
(2)Token based authentication [12]
(3)PUF based authentication [17]
(4)Context based authentication [11]
(5)Procedure based authentication

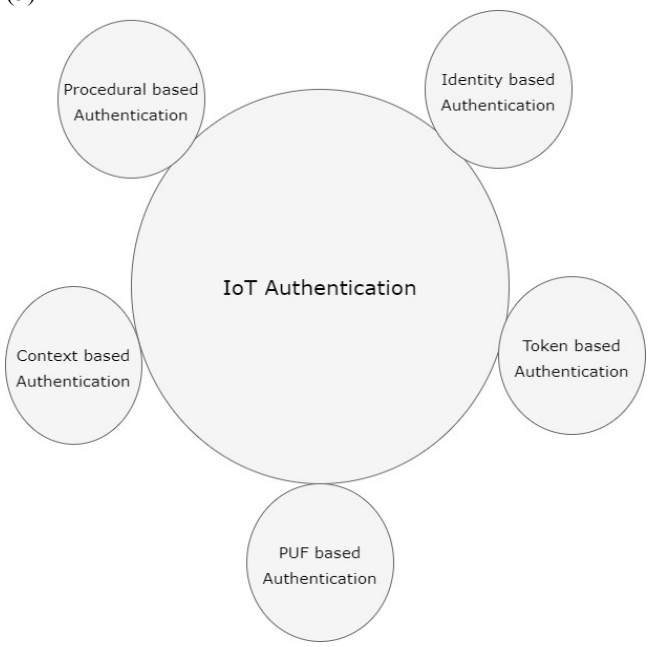

Fig 1: IoT Authentication Approaches

Each of these approach has its own advantages & dis-advantages. Identity based authentication approach consider password/ key value for validating identity. These information is already stored into device memory at the time of manufacturing. So, if an intruder can get access of device, cloning of device can be made easily or intruder can derive password/ key value from memory by power analysis attack. So, it is not advisable approach. Token based authentication works on the principal of piece of code-token issued by Authorization server to IoT device after verifying its identity. However, once after issuing token to that particular IoT device, Authorization server will not in a role during further communication. If granted token will be captured by other malicious device, it can misuse this token and by providing that token to the Resource server, illegally it can become member of network and can launch other attacks also. Physical Unclonable function does not require to store anything into device memory for authentication purpose. However, it works based on the Challenge- Response mechanism. Server will provide some challenge to the device and device will compute the response for that challenge. For computing the response, Integrated circuit is already designed and built in the device. Server will verify the response and if it is valid then device will be authenticated. However, it is also vulnerable to Modeling threat which is innovated recently. And also it does not take into account environment parameters for computing Challenge-Response pair. It is not possible that every time for the same challenge; same response will be generated. Context based authentication approach takes into consideration Physical and Behavioral context parameter for authentication. However, behavioral parameter can be copied easily. So, it will not provide accurate result for authentication. Different devices can have same operational behavior while solving assigned tasks. Procedural based authentication can be one way authentication or mutual authentication. Mutual authentication is beneficial for better security as in that type both parties involved in communication, will authenticate each other and then they will establish session for data exchange.

3. RESEARCH GAP

(1) Existing Authentication approaches for IoT system are based on a single shared key or password to authenticate IoT device. But these methods are prone to the various security threats- Key stolen attack, Side channel attack, MITM attack, Device cloning attack. If the key or password value does not updated over the peiod of time, then it will leads towards Dictionary attack. And if the third party has the access of password or key, he/ she can make an identical fake device. Because of that designed authentication approach should be dynamic in nature, in which key value should be changed according to session time period “One Session, One Cipher”. Advantage of such approach will be that if adversary gets shared key or password than also he/she can not enter into the system and can not damage to the system security. Also we can offer protection against some well-known security threat-Dictionary attack, MITM attack.

(2) We know that most of IoT devices are placed at locations which are very much critical for decision making process. If an adversary gains access of that device, he/ she can modify its location and then device will transfer fake/ malfunctioned data to the base command and control center. Because of that damage can be take place in the system. If we take example of sensor devices which are placed at road, measuring speed of vehicles passing from that road and transferring these measured information to base command center for taking further important decision.

Now, if an intruder spoofed with location of that sensor device, now, device will transfer false information to the command center and command center will take decision based on these false information. It can leads to accident and congestion also. In this type of situation, a conventional password-based or secret-key based authentication approach, which considers a shared secret key/ password is the only authentication factor, is not good solution for solving the security related problems. It will provide device authentication in ambiguous way. Also it opens a door for various Physical attack- Device stolen attack and changing distance attack. So, we should also consider context parameter for device authentication. It will tighten security and enhance authentication process.

4. OPEN PROBLEM STATEMENT

To design efficient IoT Authentication approach by considering multi-parameters (1) Physical Context (2) Multi-key parameter in which key value should be updated according to session time. Designed approach will offer security against threats such as Key Stolen threat, Monitoring threat, MITM threat and Changing distance threat. It will also identify requests from intruder at early stage of communication and will improve the system performance in terms of latency and throughput.

5. ADVANTAGES OF CONTEXT & DYNAMIC KEY PARAMETER FOR IoT AUTHENTICATION

Context Parameter: If any contextual variable like location information is checked at the time of the login session, the request messages from intruders can be identified at early stage, and after that there is no requirement of verifying other factors during the authentication session unnecessarily. It will help to enhance the performance of the security system in terms of delay.
Dynamic Key Parameter: As we know that if same key will be used for long duration of time for authentication purpose, it will provide opportunity to an intruder to launch Key stolen and monitoring attack. So, it is better to modify and update key value regularly according to session time. So, if an Intruder gets access of key; then also, he/ she will not get success in capturing session key for future communication. So, it will provide protection against Key stolen and monitoring attack.

TABLE II: Parameters/ Methods can be used for Problem Statement Solution

Sr. No.	Parameter/ Method	Advantages
1	Context Information (Physical/ Behavioral)	-Context Based Authentication -Prevention against Location spoofing attack.(Useful in applications such as Military, Industry where location of a device is also prime concern with identity).
2	Dynamic Key (Random Number/ Physical Property based/ Vault based)	-Dynamic Key Based Authentication -Prevention against Key Stolen and Monitoring attack. -Session key will be generated securely & dynamically by using any of parameters suggested in Parameter/ Method.

TABLE III: Findings from Existing Approaches of Context based / Dynamic Key based Authentication methods

Sr.No.	Author	Proposed Technique	Finding
1	Lin Wang et al. (2020)	Dynamic Key Generation techniques based on Physical Properties of device	-The generation of symmetric key by using the physical layer information such as Channel State Information & RSSI in wireless communication. -Key will not be updated in each session as Physical parameters will not change frequently.

2	Lukas Nemec et al.(2019)	Dynamic approach for Key Re-establishment into WSN	-Key establishment from Radio channel properties- RSS. - If the principal of Spatial de-correlation is violated mean Adversary is present in nearby distance of transmitting device, then adversary will also get same RSSI value and he/ she can get the same key.
3	Alan J. Michales et al. (2019)	PRNG based Key Derivation Functions for Dynamic Key Generation	-Linear Feedback Register circuit is used for PRNG. -Linear and Deterministic in nature. Does not provide good randomness.
4	Mortiz Loske et al. (2019)	Context based Authentication	-Physical/ Behavioral context parameters are suggested for IoT Authentication. -RSSI & Device operation capability do not provide unambiguous results for device Authentication.

6. CONCLUSION

IOT consists of collection of various physical devices in which they can exchange the data without any interruption. These devices are directly connected to the web and web operates in open environment. So, it provides a chance to intruder for performing different cyber-attacks. IOT Security is prime research domain for researchers of academics and industry. IOT security focuses on CIA Model- Confidentiality, Integrity and Authentication. We have reviewed challenges which are present till yet in IOT Architecture followed by necessity of authentication into system. We have identified related research gap which is still present for providing a complete IOT security solution. We have identified open research statements on which various researchers can contribute their knowledge for offering precise and efficient security solution.

References

[1] Santhosh Krishna B V, Gnanasekaran T.: A Systematic Study of Security Issues in Internet-of-Things (IoT), presented at IEEE International conference on I-SMAC (2017).

[2] Chang-le Zhong, Zhen Zhu, Ren-gen Huang. C: Study on the IOT Architecture and Access Technology, presented at IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (2017).

[3] Vangelis Gazis, Manuel Goertz, Marco Huber, Alessandro Leonardi. C: IoT: Challenges, Projects, Architectures, presented at IEEE 5th International Conference on Intelligence in Next Generation Networks (2015).

[4] Jeffry Voas, Bill Agresti. T: A Closer Look at the IOT "things", published in IEEE Computer Society, Vol. 20, Issue 30, pp. 6-15 (2018).

[5] SulabhBhattarai,Yong Wang. T: End-to-End Trust and Security for Internet of Things Applications", published in IEEE Computer Society (2015).

[6] Mardianabinti Mohamad Noor, Wan Haslina Hassan. T: Current research on Internet of Things (IoT) security: A survey, published in ELSEVEIR Computer Networks, pp. 283-294 (2019).

[7] Tarak Nandy, Norjihan Abdul Ghani, Sananda Bhattacharya. T: Review on Security of Internet of Things Authentication Mechanism, published in IEEE Access, Vol. 7, pp. 151054- 151089 (2019).

[8] Hokeun Kim, Edward A. Lee. T: Authentication and Authorization for the Internet of Things, published in IEEE Computer Society (2017).

[9] Hirofumi Noguchi, Misao Kataoka, Yoji Yamato. T: Device Identification Based on Communication Analysis for the Internet of Things, published in IEEE Access (2019).

[10] Mohammad Wazid, Ashok Kumar Das, VangaOdeluc et al T: Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, published in IEEE Internet of Things Journal (2017).

[11] Ning Wang, Ting Jiang, Shichaolyet al. T: Physical-Layer Authentication Based on Extreme Learning Machine, published in IEEE Internet of Things Journal, (2016).

[12] Muhammad Naveed Aman, Sachin Taneja et al. T: Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff, published in IEEE Internet of Things Journal (2015).

[13] Prosanta Gope, Biplab Sikdar. T: Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices, IEEE Internet of Things Journal, (2018).

[14] Muhammad Naveed Aman, Mohamed Haroon Basheer, Biplab Sikdar. T: Two factor Authentication

for IOT with Location Information, IEEE Internet of Things Journal (2017).
[15] Yan Zhao, Shimming Li, Liehui Jiang. T: Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment, WILEY Hindawai Security and Communication Networks, (2015).
[16] Majid Alotaibi. T: An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN", IEEE Access (2015).
[17] Zahoor Ahmed Alizai, Noquia Fatima Tareen, Iqura Jadoon C: Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures, IEEE International Conference on Applied and Engineering Mathematics (2015).
[18] Vikas Hassija, Vinay Chamolaet al. T: A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, published in IEEE Access (2019).
[19] Jyoti Deogirikar, Amarsinh Vidhate T: Security Attacks in IoT: A Survey presented at IEEE International conference on I-SMAC (2017).
[20] Chang-le Zhong, Zhen Zhu, Ren-gen Huang. C: Study on the IOT Architecture and Access Technology, presented at IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, (2017).
[21] Daniel A.F.Saravia, Paul Crocker. T: PRISEC-Comparison of Symmetric key algorithms for IOT, Sensors (2019).
[22] Lin Wang, Zhou Chang. T: Security Enhancement on a Light Weight Authentication Scheme with Anonymity Fog Computing Architecture, Vol.8, IEEE Access (2020).
[23] Yuichi Kawamoto, Hiroki Nishiyama T.: Effectively Collecting Data for the Location-Based Authentication in Internet of Things, IEEE System Journal, (2015).
[24] Omar Alfandi, Arne Bochem. T: Secure and Authenticated Data Communication in Wireless Sensor Networks, Sensors (2015).
[25] Adel Ali Ahmed, Waleed Ali Ahmed. T: An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things, Sensors (2019)