International Journal of Engineering, Science and Mathematics
Vol. 13 Issue 2, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

SURVEY: SECURITY ISSUES AND CHALLENGES FOR AUTHENTICATION OVER IOT NETWORKS

Rohit Sharma*, Kapil Kumar Kaswan**
****Mtech Scholar, CSE Department, CDLU,Sirsa , India***
***** Assistant Professor, CSE Department, CDLU,Sirsa , India***
rsrohitsharma206@gmail.com, **kapilkaswan@gmail.com

ABSTRACT

IoT network can be deployed in various domains i.e. healthcare, industry, agriculture, smart homes, military, surveillance etc. Differentdevices such as sensors, actuators, machines, industrial robots etc. can exchange the data over open network. In such case, authentication of intermediate nodes is quite challenging as well as data can be intercepted during transmission. To prevent the unauthorized to network resources, it is necessary to authenticate the nodes. In this paper, various constraints related to authentication over IoT network will be explored.

***Keywords**-Authenticate, Authorization, IoT Security, Threats, Intrusion*

I. INTRODUCTION

Internet of Things (IoT) enables the machine to machine communication and it supports data exchange between different types of devices i.e. sensors/mobile phones/computers/robots etc. Transmission over heterogeneous environment may invite the intruders those can capture the network traffic to launch the threats. Following are the common threats for IoT networks:

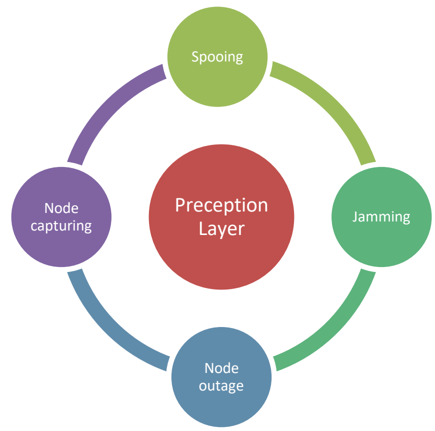

Figure: 1 Security threats for preception layer

Figure 1 shows the security threats for preception layer and these are signal jamming/nodeoutage/capturing/spoofing etc.

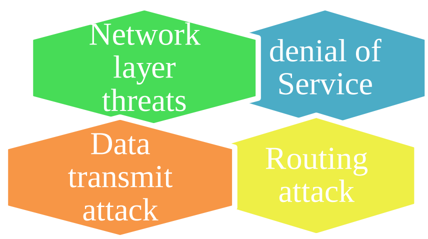

Figure: 2 Network layer atatck

Figure:2 shows the network layer threats and it includes denial of service/data transmmit attack/routing atacks etc.

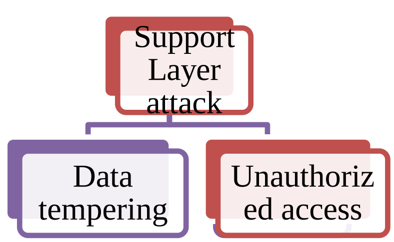

Figure 3: Support layer attack

Figure 3 shows the different types of support layer atatcks that includes data temering and unauthorized access to network resources.

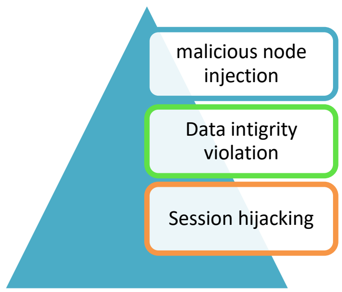

Figure 4: Application layer attack

Figure 4 shows various types of atatcks those can be launched over application layer snd it includes malicious node injection/intigrity voilation and session hijacking etc.

Challenges for security provisions

- Device authentication in hetrogenious environment is quite complex
- Identifiction of trusted devices over network is another issues
- Compatibility issues of traditional cryptography methods with IoT devices
- Key calculation may consume excessive resources over IoT network
- Quite difficult to develop a single security solution of entire IoT network due to hardware/software compatibility concerns.
- Key management at large scale IoT network is another issue.

Security Goals

There is need to:

- devlop a zero trust based security provision for IoT devices.
- Optimize the cryptography methods to minimize resource consumption/computational overhead etc.
- ensure hardware and software compatibilty by adapting universal standards.
- devlop a single security framework to secure the IoT network from multiple threats

security provision must able to secure the network under the constraints of cross layer atatcks. [1-5]

II. LITERATURE SURVEY

U. Chatterjee et al. [6] used Elliptical curve cryptography (ECC) method to secure the communication over IoT networks. Experiments show that it offers lightweight authentication and key management process that consumes less network resources (under the constraints of compromised network) as compared to existing schemes.
Q. Ma et al. [7] developed an authentication scheme for smart home appliances. It uses device signatures for the authentication the neighbors over IoT network. Analysis shows that intermediate devices can authenticate each other to ensure the secure communication against forging attack.
Y. Li [8] developed a multi-factor authentication scheme for IoT networks using ECC cryptography. It uses a real-random model for security and it also calculates the trust factor on the basis of device signatures. Analysis indicates that it is more secure/resource efficient as compared to existing authentication schemes.
R. Krishnasrijaet al. [9] developed a polynomial based authentication process for IoT networks. It uses session keys for device authentication. Simulation results show that it can guard the network resources against common security threats as well as it has less computational overhead.
Z. Wang et al. [10] introduced a lightweight authentication scheme for IoT networks. It assigns unique id (based on the device hardware) to each device in the network and after that a centralized server is used to register the devices for secure communication. Analysis show that it consumes less computational resources as compared to existing schemes.
A. G. Mirsaraei et al. [11] integrated the ECC method with blockchain technology for the smart card based authentication over IoT networks. It uses a private trusted server for blockchain based user registration. Analysis shows that it outperforms in terms of computational overhead/energy consumption.
P. Tyagi et al. [12] investigated the issues related to multi-factor authentication scheme. Study shows that it is less secure against man-in-middle attack as session keys can be compromised at intermediate device level. Analysis data can be further utilized to overcome from the shortcoming of this scheme.
Z. Siddiqui et al. [13] integrated the digital certificate based authentication over IoT networks using a centralized server. Experiments show that it is highly efficient scheme as compared to existing schemes (Prosanta/Biplab authentication).

Z. Wang et al. [14] proposed a key agreement protocol for device authentication using third party centralized server that is responsible to distribute/manage the keys for each device. Analysis shows that it is more robust as compared to existing scheme (mutual identity).
Y. Zheng et al. [15] introduced an end point authentication protocol for IoT networks. It integrates fuzzy logic for key generation/distribution/management. Analysis shows its resistance against common threats (man-in-middle/ replay attack) as well as it consumes fewer resources as compared to existing methods.

III. RESEARCH GAPS

Researchers investigated the few common threats over IoT networks i.e. replay attack/man-in-middle attack etc. and developed various authentication schemes to identify the legitimate devices over the network. As per study, it can be stated that IoT devices are low powered and lightweight cryptography methods are required as traditional security provision are not compatible with such type of devices due to excessive computational overhead as well as these methods also consumes extra resources. Current investigation indicates that there is need to optimize the cryptography methods in terms of computations/energy consumption/bandwidth usage as well as there should be a provision to encounter the threat under the constraints of compromised network.

IV. CONCLUSION

Current study explored the different provisions to secure the communication over IoT network. It can be observed that authentication and authorization both are critical facts because it is quite hard to recognize the devices over heterogeneous/open network environment. Researchers developed various solutions to strengthen the IoT security. It includes the different protocols i.e. end point authentication protocol and key agreement protocol. Researches also proposed authenticationusing digital certificates, multi-factor, lightweight blockchain method, polynomial based, smart device verification and efficient key management scheme etc.
In future, it will be extended to provide the secure communication over other networks i.e. Wireless sensor networks/Mobile ad hoc networks etc.

V. REFERENCES

[1] P. P. S, P. Durgadevi, "Systematic Analysis of Tools Employed in Threats Detection in Iot Environment," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, IEEE-2022, pp. 1-10.

[2] S. Ghosh, A. Zaboli, J. Hong and J. Kwon, "An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System," in IEEE Access, vol. 11, pp. 14752-14777, 2023
[3] M. S. Sharbaf, "IoT Driving New Business Model, and IoT Security, Privacy, and Awareness Challenges", IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, IEEE-2022, pp. 1-4.
[4] S. N. Swamy, D. Jadhav, N. Kulkarni, "Security threats in the application layer in IOT applications", International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), IEE-2017, pp.477-480.
[5] S. Jain, V. Lakshmi, R. Srivathsa, "IoT and OT Security Handbook: Assess risks, manage vulnerabilities, and monitor threats with Microsoft Defender for IoT", Packt Publishing, IEEE-2023.
[6] U. Chatterjee, S. Ray, S. Adhikari, M. K. Khan, M. Dasgupta, "An improved authentication and key management scheme in context of IoT-based wireless sensor network using ECC", Computer Communications, Vol.209, Elsevier-2023, pp.47-62.
[7] Q. Ma, H. Tan, T. Zhou,"Mutual authentication scheme for smart devices in IoT-enabled smart home systems", Computer Standards & Interfaces, Vol.86, Elsevier-2023, pp.1-16.
[8] Y. Li,"A secure and efficient three-factor authentication protocol for IoT environments", Journal of Parallel and Distributed Computing, Vol.179, Elsevier-2023, pp.1-23.
[9] R. Krishnasrija, A. Kr. Mandal, A. Cortesi, "A lightweight mutual and transitive authentication mechanism for IoT network", Ad Hoc Networks, Vol.138, Elsevier-2023, pp.1-12.
[10] Z. Wang, J. Huang, K. Miao, X. Lv, Y. Chen, B. Su, L. Liu, M. Han, "Lightweight zero-knowledge authentication scheme for IoT embedded devices", Computer Networks, Vol.236, Elsevier-2023, pp. 1-19.
[11] A. G. Mirsaraei, A. Barati, H. Barati, "A secure three-factor authentication scheme for IoT environments", Journal of Parallel and Distributed Computing, Vol. 169, Elsevier-2022, pp.87-105.
[12] P. Tyagi, S. Kumari, "Security Flaws in Dhillon and Kalra's User Authentication Scheme for IoT", 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, IEEE-2022, pp. 1-4.
[13] Z. Siddiqui, J. Gao, M. Khurram Khan, "An Improved Lightweight PUF–PKI Digital Certificate Authentication Scheme for the Internet of Things", IEEE Internet of Things Journal, Vol.9 (20), IEEE-2022, pp.19744-19756.
[14] Z. Wang, P. Sun, N. Luo, B. Guo, "A Three-Party Mutual Authentication Protocol for Wearable IOT Health Monitoring System", IEEE International Conference on Smart Internet of Things (SmartIoT), Jeju, Korea, Republic of, IEEE-2021, pp.344-347.

[15] Y. Zheng, C. -H. Chang, "Secure Mutual Authentication and Key-Exchange Protocol between PUF-Embedded IoT Endpoints", IEEE International Symposium on Circuits and Systems, IEEE-2021, pp.1-5.