International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 5th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 01

DOI: 10.48047/IJIEMR/V12/ISSUE 01/15

Title **A Survey on Overview of Security Protocols, Mechanisms, Attacks, Applications Suitable For IOT Devices Over Wireless Networks**

Volume 12, ISSUE 01, Pages: 152-160

Paper Authors

SATISHA C, Dr RAGHAV MEHRA

A Survey on Overview of Security Protocols, Mechanisms, Attacks, Applications Suitable For IOT Devices Over Wireless Networks

SATISHA C[1], Dr RAGHAV MEHRA[2]
[1]Research Scholar, Department of Computer Science, Bhagwant University, Ajmer, satisha.chandra@gmail.com
[2]Associate Professor & Assistant Director, BIT-Bhagwant Institute of Technology, Muzaffarnagar, raghav.mehrain@gmail.com

Abstract
IOT is an emerging field of research, merging IOT with other devices like sensors may use protocols and technologies of sensor networks, which leads development of new sensor devices, and IOT are used in many applications of our day to day life activities to monitor. IOT devices are used in many application, smart houses, smart vehicles, transportation, health care, grids and all these applications need a specific security requirement. IOT also merged with different types of hardware devices, network protocols, and network services. Protecting IOT devices are one of the important challenging tasks. In this research paper, we conducted detailed survey on various layers of IOT devices security attacks, taxonomy of various security attacks on network layer, transport layer, perception layer, protocol layer, and application layer, and applications of IOT devices. Compared different techniques proposed by previous researcher on IOT devices security to provide security solutions like authentication, integrity, privacy, confidentiality, and access control.

Keywords: *IOT devices, Security techniques, taxonomy of security attacks, applications, attacks on IOT layers, advantages and limitations of IOT, ZIGBEE, DDS, SIGFOX.*

1. Introduction

In 1999, IOT is invented, day by day it is increased popularity, and now a day's used in many applications. IOT is a collection of devices or things that are used to gather data from applications and send to other nodes in an application [9]. IOT enhanced internet technologies and are used to provide connection between peoples over a wireless network, and end users connected through IOT devices. IOT devices gather data first, preprocess collected data, and analyze data for any decision making process. IOT devices may decrease the human presence, act like a person and this will help us to reduce manpower and which in turn help us to live comport life [17].

IOT is a one of the fast growing field and in future it will be used in almost every application in the world. Authors in [5] conducted survey on IOT and up to 2021 approximately fifty billion IOT devices are using in the world to connect over a wireless network. IOT devices are used in many application, smart houses, smart vehicles, transportation, health care, grids and all these applications need a specific security requirement [18].

IOT devices may used in corporate offices, homes, marts, stations, hospitals, security is limited in IOT devices which leads to lose personal information, and attackers steal IOT data to force variety of attacks [20]. For example, hackers may first gain control of smart homes and monitor all functions of users, gain control over locking system, enter into houses without any alarm signals, and steal many valuables like cash, gold, articles, and so on. In hospital IOT devices are used to monitor health conditions [22]. For example, IOT devices are deployed into human body to continuously monitor diabetic patient to pump insulin based on sugar levels, attackers hack hospital data, gain control over IOT devices data, gain control of insulin pumping system, change insulin dosage, and it may threat lives of diabetic patients. Main constraints of any IOT device are battery, limited computing capability, and security. Because of these reasons, providing security to IOT devices is essential, difficult, and gives many security challenges. More research to be done on IOT devices security area to provide more security mechanisms.

2. Related Work

IOT devices are connected to WWW, it is uniquely identifiable device, merging with sensor technologies, need to support all types of network protocols, capable to compute, able to analyze data, and provide various types of services [9]. IOT devices are fixed in other devices and some of them are tube lights, switches, doorbells, appliances, and so on. IOT devices are broadly classified into nine categories, health care devices, agriculture devices, environment monitoring devices, house products monitoring devices, utility devices, products for supply chain, devices for industries, devices for transport system, and manufacturing products [12].

IOT is a fast growing area of research where huge numbers of devices are connected over internet and parallel world is facing the issue of cyber crimes [6]. IOT devices may used in corporate offices, homes, marts, stations, hospitals, security is limited in IOT devices which leads to lose personal information, and attackers steal IOT data to force variety of attacks Protecting any kind of network device is a challenging task over internet, attackers may do cryptanalysis and force various types of security attacks like DDoS, attack on software, attack on data, attack on network devices, MIM attack, spoofing, malicious attacks, and so on [4].

3. Comparative Study

IoT is one of the popular devices used in many applications. Now attackers are also so closed on IoT devices to hack valuable information and providing security to IoT is a challenging task. Security of IoT device data is important which can be provided physically at sensor mode, communication to sensor devices, and communication of sensor devices. In addition to conventional security mechanism, all operation of sensor devices like transmission, receivers and calculations should be monitor carefully. Mechanisms to be developed to check and monitor sensor devices should be hacked or tampered or stolen. List of attacks possible to force at application layer, and perception layer are listed in Table1.

	Attacks On		
	Application Layer	Network Layer	Perception Layer
Fake data insertion	no	no	yes
Phishing	yes	no	no
Sniffing	yes	no	no
Sink hole	no	yes	no
Spoofing	no	yes	no
Capturing of nodes	no	no	yes
Unauthorized access	no	no	yes
DOS	no	yes	no
Malicious attacks	yes	no	no
Malicious virus	yes	no	no
Attack on battery		yes	no
Attack on Protocols	no	yes	no

Table 1: List attacks on IOT layers

Security attacks on IoT devices are broadly classified into two categories, one is attacks forced on IoT device data, and second is attacks forced on protocols used IoT channels. IoT data attacks, attacks forced to hack original, messages and packets passing via IoT devices, DOS, hash code attacks, attack on sensitive data, and create virtual machine (VM) to force malicious attack and these examples of IoT data attacks. IoT channel attacks, classified into two categories, one is attacks on communication on protocols and second one is attacks on network protocols. Channel attacks on IoT network protocols, attacks are forced at the time of establishment of connections between network nodes, sniffing, warm whole attacks, and SF attacks are example of attacks. Channel attacks on IoT communication protocols, attacks are forced when the data is transmitting between network nodes, flooding, sniffing, attacks on shared key and shipping of SSL are examples of attacks. Taxonomy of security attacks on IoT is shown in Figure1.

IOT security is a challenging task, day to day architecture of network topologies changes, architecture of gateway devices changes and need to develop security techniques like encryption, authentication, access control, and so on. List of communication protocols like SIGFOX, Data Distribution service (DDS), ZIGBEE, Bluetooth, Constraint application protocol, are used for providing communication between IOT devices. DDS protocols, is a IOT communication protocols used to provide communication between end to end system, it is a broker less protocols, used multicasting techniques to transfer information, and used to transfer data from IOT device to cloud. Bluetooth protocol is widely used, more suitable for IOT communication and consume less power. CAP protocol, more number of constraints are used in network, capable to handle congestion control, and more suitable for smart application. Some list of communication protocols used in IOT field is listed in Table 2.

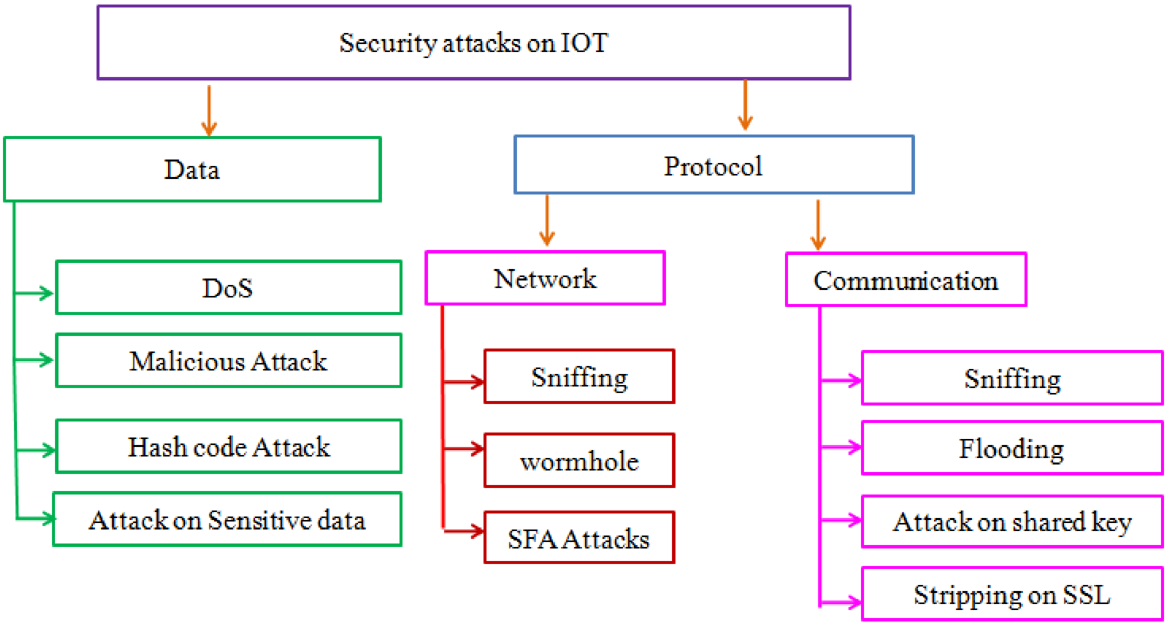

Figure 1: Taxonomy of IOT security attacks

S. No.	Communication protocols	Advantages	Limitations
1.	SIGFOX	-Useful for Wi-Fi and cellular network. -Power consumption is low. -Provide cloud accessibility. -Access controlled at end to end.	-Poor security for IOT.
2.	DDS	-High performance. -High scalability. -Good data transfer data between devices.	-DDS attack, MIM attacks possible.
3.	ZIGBEE	-More flexible. -Simulation cost is low. -Low power consumption.	-Worm hole attacks, and sink hole attacks DDoS Attacks
4.	Bluetooth	-Low power consumption. -Suitable for devices which are consuming.	-Interception. -Attacks on data during transit.
5.	CAP	-Useful for small size network. -Suitable for constraint network devices.	-DDoS attacks.

Table 2: List of communication protocols used in IOT field

IOT is gain popularity, now IOT is integrated with cloud to provide services, IOT are used in many commercial application like smart homes, automation of houses, smart laboratories, e-vehicles, and so on. From survey we came to know that IOT is one the device to force attacks to hacked information. Addressing IOT security is one the challenging task. Traditional security algorithm faces issues like compatibility of IOT technology and consumption of high power to perform task, and so on. We conducted survey on few research articles, list of algorithm use to solve IOT security issues and security mechanism supported by each algorithm is listed in Table 3.

	[2]	[7]	[8]	[10]	[14]	[15]
Trust management	no	no	no	yes	yes	no
Privacy	no	no	yes	no	no	no
Authentication	yes	yes	no	no	no	no
Availability	no	no	no	no	yes	no
Confidentiality	no	no	yes	yes	no	no
Integrity	yes	no	yes	no	no	yes

Table 3: Security issues faced by algorithms

Providing security to IOT devices data is not an easy task, IOT is one of the latest trending research area and to fill the security gap researchers produced variety of techniques. All traditional algorithms on IOT security covers security on IOT data, IOT communications, and IOT devices but single algorithm is not appropriate to restrict all types of attacks. IOT devices are used in many application, smart houses, smart vehicles, transportation, health care, grids and all these applications need a specific security requirement. For example, in health care privacy is essential and in smart cities authentication is required. In this research, we studied number of security algorithms related to IOT and all these algorithms address IOT security issues like authentication, integrity, key exchange, confidentiality and privacy in table listed. List of techniques protect against main in the middle attack, masquerade attack, eavesdropping attack, spoofing attack, birthday attack, impersonation and synchronization attack. In table 4 shown lists of algorithms resist various attacks.

	[1]	[3]	[4]	[6]	[11]	[12]	[13]	[16]	[19]	[21]
DOS attack	yes	no	yes	no	yes	no	yes	yes	yes	no
MIM	no	yes	no	no	no	no	yes	no	no	no
Replay attack	no	yes	no	no	yes	yes	no	yes	yes	yes
Masquerade attack	no	yes	no	no	no	no	no	no	yes	no
Battery drain attack	no	no	yes	no	no	no	no	no	no	no
Eaves dropping	no	no	no	no	yes	no	yes	no	no	no
spoofing	no	no	no	no	no	yes	no	no	no	no
Birthday attack	no	no	no	yes	no	no	no	no	no	no
Impersonation attack	no	no	yes	no	no	no	no	no	no	no
synchronization attack	no	no	no	no	no	no	yes	no	no	no

Table 4: Methods resist various security attacks

4. Conclusion

IOT is an emerging field of research, merging IOT with other devices like sensors may use protocols and technologies of sensor networks, which leads development of new sensor devices, and TOI are used in many applications of our day to day life activities to monitor. IOT is a fast growing area of research where huge numbers of devices are connected over internet and parallel world is facing the issue of cyber crimes. In this research paper, we conducted detailed survey on various layers of IOT devices security attacks, taxonomy of various security attacks on network layer, transport layer, perception layer, protocol layer, and application layer, and applications of IOT devices. Compared different techniques proposed by previous researcher on IOT devices security to provide security solutions like authentication, integrity, privacy, confidentiality, and access control.

References

Lee, C., Fumagalli, A., "Internet of Things Security–Multilayered Method for End-To-End Data Communications Over Cellular Networks", Proceeding Of IEEE 5th World Forum Internet Things (WF-Iot), Limerick, Ireland, Pp. 24–28, 2019.

Lv, P., Wang, L., Zhu, H., Deng, W., Gu, L., "An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Block Chains", IEEE Access, vol. 7, pp. 41309 - 41314, 2019.

Sopori, D., Pawar, T., Patil, M., Ravindran, R., "Internet of Things: Security Threats", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 6, No. 3, Pp. 263-267, 2017.

Jain, A., Sharma, B., Gupta, P., "Internet of Things: Architecture, Security Goals, and Challenges - A Survey", International Journal of Innovative Research in Science and Engineering, vol. 2, no. 4, pp. 154-163, 2016.

Kausar, F., Alzaydi, S., Aljumah, S., Alroba, R., "Traffic Analysis Attack For Identifying Users' Online Activities", IEEE IT Professional, vol. 21, no. 2, pp. 50-57, 2019.

Taghanaki, S.R., Jamshidi, K., Bohlooli, A., "DEEM: A Decentralized and Energy Efficient Method for Detecting Sinkhole Attacks on The Internet of Things", In IEEE, Mashhad, Iran, Iran, 2019.

Fernandez, T.M., Fraga Lamas, P., "A Review on the use of Block chain for the Internet of Things", IEEE Access, vol. 6, pp. 32979-33001, 2018.

Alotaibi, A., Barnawi, A., Buhari, M., "Attribute based Secure Data Sharing with Efficient Revocation in Fog Computing", Journal Of Information Security, vol. 8, pp. 203-222, 2017.

Frustaci, M., Pace, P., Aloi, G., Fortino, G., "Evaluating Critical Security Issues of The IOT World: Present and Future Challenges", IEEE Internet Things Journal, vol. 5, no. 4, pp. 2483-2495, 2018.

Abbas, N., Zhang, Y., Taherkordi, A., Skeie, T., "Mobile Edge Computing: A Survey", IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450 - 465, 2018.

Lundqvist, T., De Blanche, A., Andersson, H., "Thing to thing Electricity Micro Payments Using Block chain Technology", In Proceedings of IEEE Global Internet Things Summit, pp. 1-6, 2017.

Premsankar, G., Di Francesco, M., Taleb, T., "Edge Computing for The Internet of Things: A Case Study", IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1275 - 1284, 2018.

Shae, Z., Tsai, J., "On the Design of a Block chain Platform for Clinical Trial and Precision Medicine", In Proceeding of IEEE 37th International Conference on Distributed Computing Systems, pp. 1972-1980, 2017.

Christidis, K., Devetsikiotis, M., "Block chains and Smart Contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292-2303, 2016.

Razzaque, M.A., Milojevicc, M., Palade, A., Clarke, S., "Middleware for Internet of Things: A Survey", IEEE Internet Things Journal, vol. 3, no. 1, pp. 70-95, 2016.

Xiao, L., Xie, C., Chen, T., Dai, H., Poor, V., "A Mobile off loading Game against Smart Attacks", IEEE Access, vol. 4, pp. 2281 - 2291, 2016.

Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H., "A Survey on Security and Privacy Issues in Internet of Things", IEEE Internet Things Journal, vol. 4, no. 5, pp. 1250-1258, 2017.

Din, I.U, Guizani, M., Kim, B.S., Hassan, S., Khan, M.K, "Trust Management Techniques for The Internet of Things: A Survey", IEEE Access, vol. 7, pp. 29763-29787, 2019.

Eckhoff, D., Wagner, I., "Privacy in the Smart City applications, Technologies, Challenges, and Solutions", IEEE Communications surveys, vol. 20, no. 1, pp. 489-516, 2018.

Xia, X., Xiao, Y., Liang, W., "ABSI: An Adaptive Binary Splitting Algorithm for Malicious Meter Inspection in Smart Grid", IEEE Transaction on Information Forensics Security, vol. 14, no. 2, pp. 445-458, 2019.

Jose, A.C., Malekian, R., "Improving Smart Home Security: Integrating Logical Sensing into Smart Home", IEEE Sensors Journal, vol. 17, no. 13, pp. 4269-4286, 2017.

Abdul-Ghani, H.A., Konstantas, D., Mahyoub, M., "A Comprehensive IOT Attacks Survey Based on a Building Blocked Reference Model", International Journal of Advanced Computer Science Applications, vol. 9, no. 3, pp. 355-373, 2018.