American Journal of
Electronics & Communication

REVIEW ON VULNERABILITIES AND CHALLENGES ON IOT SECURITY FRAMEWORKS IN DIVERSIFIED FIELDS OF APPLICATIONS

Poojarini Mitra
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
poojarini.mitra@uem.edu.in

Kaustuv Bhattacharjee
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
kaustuv.bhattacharjee@uem.edu.in

Anirban Das
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
anirban-das@live.com

Susmita Das
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
susmitakgp128@gmail.com

Papiya Ghosh
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
jiniaghosh96@gmail.com

Priya Gorai
Dept. of Computer Applications
University of Engineering and Management
Kolkata ,India
priyagorai31@gmail.com

Sayani Maity
Dept. of Computer Applications
University of Engineering and Management
Kolkata, India
maitysayani98@gmail.com

Abstract—Internet of Things (IoT) is emerging as a revolutionary technology since the last double decade. Internet of things has changed many aspects of the human. IoT has changed living styles and health care with the help of intelligent health care technologies like wearable devices. IoT makes use of lightweight communication with the motive of the reduction of extra overhead generated in regular internet communication. The number of multiple devices are connected and the amount of data interchanged between them is surprising and hence becoming a goal for attack and misuse of information. Other than the obvious vulnerability of wireless connections, security in IoT is difficult to earn because of the universal way of data collection, complication of cryptographic solutions for the resource-tractable equipment, characteristics of the cyber world with the physical world, complex wideness topologies and insufficient organizational capabilities. The Internet of Things (IoT) devices are becoming more popular, vulnerability counteragents are inadequate and many things have occurred. It is because there is inadequate preservation against vulnerabilities specific to IoT equipment.

Keywords— IoT, MQTT, Blockchain, Security, Systolic Inversion, 6LoWPAN, REST, dataencryption

I. INTRODUCTION

The phrase Internet of Things (IoT) refers to a network in which various physical devices and objects are connected throughout the world via internet.“Things” in the IoT sense, is the mixture of hardware, software, data and services. The term IoT was firstly announced by Kevin Ashton in 1999. IoT emerges as a revolutionary technology since last decade. With survey estimating that by 2020 there will be over 20 billion IoT devices. In the recent years, Internet of Things (IoT) have become one of the most popular techniques and expanding globally and providing diverse benefits in nearly every aspect of lives. There are plenty of IoT applications in various areas such as healthcare, automation and industrial manufacturing, electricity, smart city, agriculture, logistics, vehicular technology, retail, security, business management etc. IoT also serves for social needs such as surgery monitoring, weather condition detection, animal identification. By collecting and examining data coming from IoT devices, it is possible to raise the efficiency of the entire system. IoT allows objects to be controlled remotely across existing network infrastructure. It is a very good technique which reduces human effort as well as easy access to physical devices. This technique also has autonomous control feature by which any device can control without any human interaction.

IoT security-IoT security covers both physical device security and network security, and impacts the processes, technologies, and measures necessary to protect IoT devices and networks. It spans industrial machines, smart energy grids, building automation systems, entertainment devices, and more, including devices that often aren't designed for network security. IoT device security must protect systems, networks, and data from a broad spectrum of IoT security attacks. A robust IoT security portfolio allows developers to protect devices from all types of vulnerabilities while deploying the security level that best matches their application needs. Cryptography technologies help combat communication attacks, while security services can protect against lifecycle attacks.

II. RELATED SURVEY

There are various existing works on IoT security and privacy issues. With the current anomalous research interest in IoT, many new protocols are being ascertain every year.

A. MQTT SECURITY FRAMEWORK IN GENERIC IOT MODEL

Chintan Patel, Nishant Doshi(2020) discussed that MQTT is a publish-subscribe-based light-weighted messaging protocol where the system consists of three main components: publishers, subscribers, and a broker. It provides the interface between applications and users at one end, network and communications at the other end[1].

It has light-weighted code footprint. It provides Bi-directional communication. It has the ability scale millions of things. It provides reliability and security. MQTT is a very light-weighted protocol so cannot support heavy pay load. It uses TCP protocol which requires more processing power and more memory. It is not easy to implement.

B. AN EFFICIENT LIGHTWEIGHT INTEGRATED BLOCKCHAIN (ELIB)MODEL FOR IOT

Sachi Nandan Mohanty,K.C. Ramya(2020) discussed that Blockchain (BC) is the backbone technology of digital cryptocurrency . The blockchain is a distributed database of records of all transactions or digital occurrence that have been evolved and impart among participating parties. BitCoin is the most popular cryptocurrency an example of the blockchain . One of the useful of Blockchain is Bitcoin. The bitcoin is a cryptocurrency and is used to interchange digital assets through online[2].

The presented ELIB model focuses on an overlay network.It introduces shared keys for the communication and processes. The overlay is included as distinct clusters to reduce overheads.

C. SECURITY OF 6LOWPAN IOT NETWORKS IN HOSPITALS

Anjali Yeole, D.R. Kaldande(2019) discussed that Trust, safety and privacy is founded over a 6lowpan network running on RPL by keeping the CPU power consumption and storage requirements under check.

6LoWPAN offers wide network which can be used by the millions of devices. It uses IPv6 protocol and hence can be routed directly to cloud platforms. It has less immunity to interference than wifi or bluetooth devices[3].

D. SYSTOLIC INVERSION ALGORITHMS FOR BUILDING CRYPTOGRAPHIC SYSTEMS BASED ON SECURITY MEASUREMENT

Haibo Yi(2020) discussed that Cryptography is essential for the security of online communication and vehicles. Post-quantum cryptography is cryptography under the assumption that the attacker has a large quantum computer.

It is virtually impregnable. It is simple to use. Error rates are relatively high. Fiber-based quantum cryptography only works over fairly short distances[4].

E. SODA: A SOFTWARE-DEFINED SECURITY FRAMEWORK

Sandra Scott-Hayward, Taejune Park(2019) discussed that the design of SODA focuses on getting a user-defined security scheme through the following: Control plane: The control plane of SODA manages network components and states. Event-driven model: SODA provides an event-driven model to invoke specific elements in the control plane. Programmable interface: Rather than direct accesses among internal components or stored states, SODA provides a programmable interface. SODA provides less possibly for data back-up. It is not suitable for weightless encryption[5].

F. SECURITY INFORMATION TRANSMISSION ALGORITHMS ON CLOUD COMPUTING

Ding Li, Wu Dong(2020) discussed that Cloud is an environment of the hardware and software resources in the data centers that provide varies services over the network or the internet to gratify user requirements. Encryption is one of the most efficient ways to earn data security and safety. Data encryption is a security scheme where data is encoded and can only be decoded by user with appropriate encryption key [6].
It provides complete data protection. Security is secured in multiple devices. It moves data securely. It maintains the integrity. It is a heavyweight application. Due to use of heavyweight, the data transfer cost is increased. Compatibility is not well good.

G. CAAVI-RICS MODEL FOR THE SECURITY OF DISTRIBUTED IOT

Sasa Pesic, Costin Badica(2020) discussed that CAAVI stands for credibility, authentication, authorization, verification, and integrity. It performs enables cooperation and efficient process handling. It performs autonomous communication. It reduces the risk of the cooperation of the third-party. The implementation result in nodes being exposed and sensitive data theft. It cannot detect the source of the attack[7].

H. SECURING IOT DEVICES USING REST API (REPRESENTATIONAL STATE TRANSFER) MIDDLEWARE

Hittu Garg, Mayank Dave(2019) discussed that REST is a form of API that widely used in the modern web, and data transfer usually takes place using JSON or XML over HTTP[3]. It is a good model for heterogeneous systems. Middleware is the "glue" that connects diverse computer system. It is a software that acts as interface between components of IoT [8].

REST is a one way connection so it does not have any building messaging protocol.

I. IOTSM: AN END-TO-END SECURITY MODEL

Joseph Bugeja(2019) discussed that IOTSM can be used by IoT organizations to formulate and perform a strategy for rising end-to-end security. MSDL model planned to reduce software maintenance cost and increase reliability. BSIMM excuses which software functions are included in an organization. SAMM helps organizations to formulate and perform strategy for application safety. Security is new to many manufacturers operating in the IoT domain. It implements secure software development life cycle (SSDLC) methodologies is challenging [9].

III. Conclusion & Future Scope

IoTs can be vulnerable to a variety of attacks. One of the fundamental mechanism is secure routing, a mechanism that allows the sensors within the network to interchange routing information and data safety. The IoT usually adopt security method based on symmetric cryptographic methods. But that too involves a lot of computation and communication.

A trust management system is able to recognize compromised nodes which have been earlier authenticated. A trust management system is a process comprising of security policies, accreditations, and trust relations aimed to tell which nodes are trustworthy and which are not. Nodes are given trust level according to their reputation in the network. Our motive will be to reveal a trust management based system for addressing attacks on IoT devices. An direction for building trust management process is such that every node is evaluated of its trustworthiness by their neighbours for which they should be under constant surveillance by their neighbours.

References

[1] Chintan Patel, Nishant Doshi,"A Novel MQTT Security framework In Generic IoT Model", Procedia Computer Science, Volume 171,2020,Pages 1399-1408,ISSN 1877-0509.

[2] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, Volume 36,2019, Pages 55-81, ISSN 0736-5853,

[3] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, Internet of Things: A survey on the security of IoT frameworks,Journal of Information Security and Applications,Volume 38,2018,Pages 8-27,ISSN 2214-2126,

[4] Haibo Yi, Systolic inversion algorithms for building cryptographic systems based on security measurement in IoT-based advanced manufacturing, Measurement, Volume 161,2020,107827, ISSN 0263-2241,

[5] MartÃn Abadi, Access Control in a Core Calculus of Dependency, Electronic Notes in Theoretical Computer Science, Volume 172,2007,Pages 5-31,ISSN 1571-0661,

[6] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, Secure integration of IoT and Cloud Computing, Future Generation Computer Systems, Volume 78, Part 3, 2018, Pages 964-975, ISSN 0167-739X,

[7] AshkanYousefpour,CalebFung,Tam Nguyen, Krishna Kadiyala,FatemehJalali,AmirrezaNiakanlahiji,JianKong,Jason P.Jue,Alloneneedstoknowaboutfogcomputingandrelatededgecomputingparadigms:A complete survey, Journal of Systems Architecture,Volume98,2019,Pages 289-330,ISSN1383 -7621

[8] Abdulhadi Alqarni, Maali Alabdulhafith, Srinivas Sampalli,A Proposed RFID Authentication Protocol based on Two Stages of Authentication,Procedia Computer Science,Volume 37,2014,Pages 503-510,ISSN 1877-0509

[9] Arwa Alrawais, Abdulrahman Alhothaily, Bo Mei, Tianyi Song, Xiaolu Cheng,An Efficient Revocation Scheme for Vehicular Ad-Hoc Networks,Procedia Computer Science,Volume 129,2018,Pages 312-318,ISSN 1877-0509

[10] Ricardo Neisse, Gary Steri, Igor Nai Fovino, Gianmarco Baldini,SecKit:A Model-based Security Toolkitforthe InternetofThings,Computers&Security,Volume54,2015, Pages60-76,ISSN0167-4048