American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)

ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Security Issues in Internet of Things: A Comprehensive Review

Muhammad Fateh Khan Sial*

Assistant Professor, Department of Electrical Engineering, The University of Lahore, Defense Road, Lahore, 54000, Pakistan

Email: fateh.khan@ee.uol.edu.pk

Abstract

IoT devices can be insecure and may not be able to defend themselves against a wide variety of security threats. This is primarily due to the reason that resources on IoT devices are limited. Standards that govern the development of these devices are not yet mature. Moreover, the design, development and deployment of the software and hardware is not at all secure. The solution to these problems is that a global mechanism should be developed that is robust for securing the IoT layers. Major bottleneck in this approach is that the resources in IoT devices are very diverse in nature, based on several technologies and protocols which make it quite challenging to develop a universal protocol to meet the security threats. These threats have been divided into low level, middle level and high level layers of IoT. In this article, various mechanisms for handling security issues at different IoT layers have been reviewed. Attacks in IoT, their implications, solutions and role of Blockchain technology to address these problems are briefly presented.

Keywords: Blockchain; IoT; security threat; protocol.

1. What is Internet of Things?

International Telecommunication Union (ITU) defines Internet of things as the network of embedded devices connected via internet (public or private network). The number of these communicating nodes may rise upto 20 billion devices by 2020 [1]. These devices collect data using sensors and disseminate this information to other network nodes over internet as shown in Fig 1. As a result, a large amount of data is generated and processed to provide dependant services.

---

* Corresponding author.

These connected devices, referred to as Things, carry sensitive personal data of their users, including their behavior and preferences. Personal privacy is at a greater risk when this data shared by specific companies could be utilized for illegal purposes. IoT nodes can be remotely configured to perform a desired functionality. Information among devices is shared using standard protocols. The connected devices range from smart wearables (like fitness monitoring devices) to large systems (like washing machines, refrigerators, security cameras etc.) connected with sensors. The data collected through these devices is used to improve overall system efficiency. Impact of IoT technology will increase in every sphere of life due to the evolution of communication technologies. The security issues inherent in these new technologies that constitute the IoT network are arising in IoTs as well [15]. IoT services can be hampered by attacks posing a threat to privacy and integrity of the data. The entire network needs to be secured from these threats. The nature of these threats is analogous to those in Computer networks, as IoT is the integration of different networking technologies and realized with networking devices having limited resources.

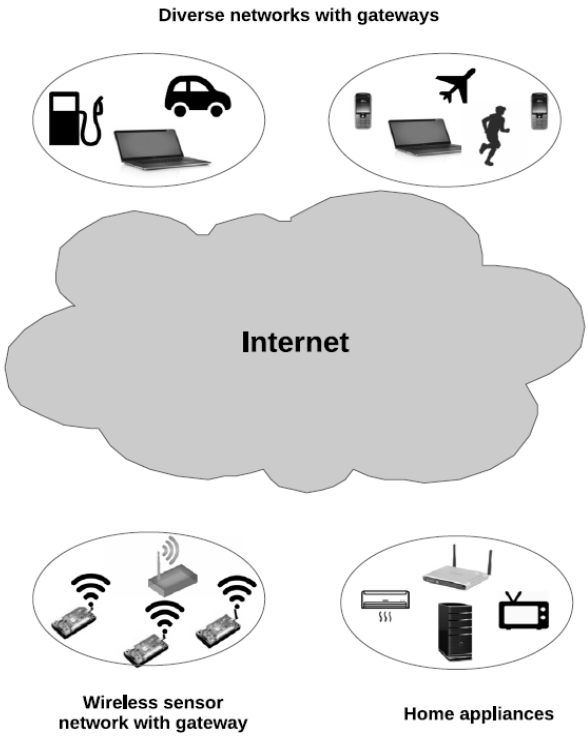

Figure 1: Components of an IoT network [2]

Different solutions have been proposed to tackle security threats in IoT network. Some approaches focus on providing end to end security others target problems at specific layer.

2. Security Issues in IoT Layered Architecture

In a typical IoT network embedded devices with sensors are connected among each other through internet. These devices are having unique identification on the network. These devices have limited memory and processing power and are connected to gateways to provide remote services to network users.

The figure 2 shows the IoT device architecture with layers of common protocols used for management, authentication, routing, messaging and applications. It includes protocols like low rate wireless personal area networks (LR-WPAN) and Low Power Wide Area Network (LP-WAN). Each device in an IoT network has a unique IPv6 address. LPWAN allows long range communication among the devices with low data rate and power. LoRaWAN protocol supports varying data rates among IoT nodes and supports communication between network nodes and gateways. Another protocol for indoor coverage is Narrow-band IoT(NB-IoT) which utilizes the spectrum of LTE [3,4,5].

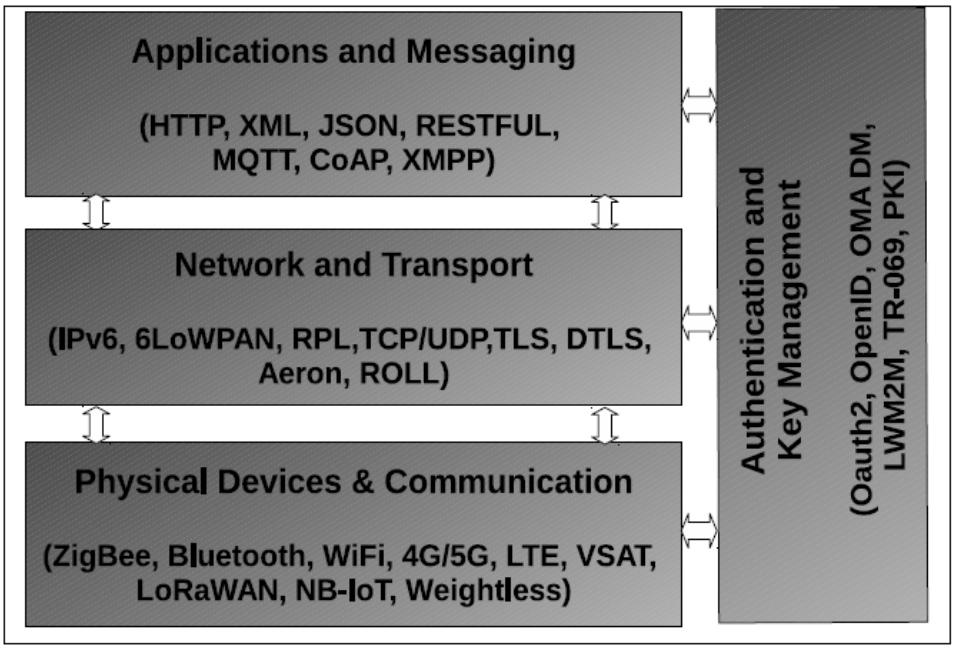

Figure 3: IoT protocols and standards [2]

3. Security requirements in IoT

There are various parameters and requirements that are needed to be considered while tackling the security requirements of IoT [15].

- Data privacy and Integrity: To make data secure as it travels longer distances by hopping among the network nodes, appropriate encryption techniques are needed to be deployed. As the network is immensely diverse in terms of devices, services and the network type, privacy of data stored in a device can be readily compromised or the data can be corrupted by the attacker.
- Authentication and authorization: Communication between two IOT nodes can be made secure by authenticating the communicating partners before starting the exchange of information. If a device wants to access privileged services, it must be authenticated first. There is a wide variety of authentication schemes available depending on the diverse architectures that support IoT networks and devices. This diversity poses a serious challenge in defining a single protocol for authentication in IoT networks. Secondly, authorization schemes must be implemented to ensure that system access or information sharing is done only to authorized user. A network can be made secure if a proper

authentication and authorization mechanism is in place. Moreover, network management can be made reliable by auditing the resource usage and report via a secure mechanism.

- Service Availability: Wide variety of attacks is possible on IoT networks which can result in temporary or long term unavailability of services. These include Denial of Service attacks, sinkhole attacks and jamming adversaries etc. These attacks are targeted at multiple IoT layers and affect the services available to end users.
- Energy Consumption: In general, IoT devices are resource-limited and possess low memory and consume low power. Attacks like flooding the network with fake connection request results in memory overruns and increased energy consumption by the network nodes.
- Single Point of Failure or Breakdown: Faults may occur causing failure at a single point in the ever expanding heterogeneous IoT network. In case of multiple single point failures taking place all over the network, can result in significant degradation in the quality of service. Therefore, it is very important to develop and implement mechanisms to build a more resilient network.

4. Classification of Security Issues

IoT security issues are divided into three levels: low level, intermediate and high level [2,3,4].

- Low level Issues: Threats related to the physical layers and Data link layer are regarded as low level issues. These include Jamming attacks, insecure device initialization, spoofing attacks, sleep deprivation attacks, poor physical interface security.
- Intermediate level Issues: Problems related to communication and routing at network and transport layers are considered to be the Intermediate level issues. Fragmentation based duplication attacks, discovery of insecure neighbours, Denial of service attacks, Buffer reservation attacks, Low power and lossy networks attack, sinkhole and wormhole attacks, device authentication and secure communication, session hijacking, attacks on location and identity on cloud based networks.
- High Level Security Issues: These issues are related to the applications running on IoT devices. These include attacks through interfaces of web, mobile, cloud, data privacy problems, insecure software and firmware attacks, middleware security problems.

5. Security Solutions

The security related problems are caused by vulnerabilities at various layers of OSI. The security solutions are developed to overcome these vulnerabilities. These solutions have been divided into low level, mid level and high level corresponding to the problems at each layer [2,5,6].

- Low level solutions: These solutions focus on the security threats at physical, hardware and link layer. Denial of service attacks are tackled by deploying solutions that are based on signal strength measurement, packet delivery ratio calculation, encoding schemes, channel estimation, data rate variation. Physical interface can be made secure by preventing software access to hardware interfaces. Sleep deprivation attacks are tackled by employing an intrusion detection system at multiple levels.

- Mid Level Solutions: Duplication attacks are prevented by introducing time stamp and fragment verification through hash chain. Insecure neighborhood problem is solved by deploying cryptography based authentication algorithm. Routing attacks are prevented by using user authentication. Denial of service by wormhole attacks are prevented by verification through hash chain functions, solutions based on signal strength measurement, cryptographic algorithms, intrusion detection system for anamoly detection and communication behaviour analysis. Attacks on privacy can be detected by maintaining list of trusted/untrusted users. Denial of service attacks caused by session establishment and resumption are solved by deploying authentication mechanism based on encryption keys.
- High level Solutions: Denial of service attacks at application layer caused by insecure interfaces, software/firmware can be prevented by making passwords stronger, test software against vulnerabilities of tools and firewalls, regular firmware updates, use of signatures and encryption algorithms. Network disruption due to middleware security and privacy violation is tackled by deploying solutions based on authentication, effective security policies and deploying encryption algorithms.

6. Blockchain Technology based Solutions

Blockchain is considered as an emerging technology that is going to play a major role in managing and securing IoT devices. IoT security challenges are of wide variety and the potential of Blockchain technology to handle them is discussed in the following.

Blockchain is a digital database that is distributed, decentralized and shared across a network. It stores record of assets and transactions in the form of blocks of data chained digitally, time stamped and validated by data miners. Data integrity is ensured by using strong cryptographic and hashing techniques. In this technology, each transaction is carried out by in the shared database by the consensus of majority nodes which are responsible for authenticating and validating transaction. After performing transaction validation, the relevant data becomes a permanent part of the database. Some of the Blockchain characteristics are shown in Fig 3. Generally, Blockchain networks are categorized into two types [12,13,14]

- Public networks: This network is open for everyone to join which in turn provides security and access control problems. These networks are also referred to as permission-less networks.
- Private networks: These networks are referred to as permissioned networks and the numbers of participants are restricted.
- Consortium networks: These networks are considered as semi-permissioned as the transactions are approved by only a few authorized nodes.

One of the most popular applications that run on a Blockchain network is Bitcoin [9]. Blockchain is the underlying technology for most of the crypto-currencies. The scope of Blockchain use-cases and applications quite broad and diverse and range from crypto-currencies to machine to machine transaction, supply chain, asset tracking, digital identity, voting, certification, record management, insurance solutions, cargo shipping, banks, supply chain systems [14].

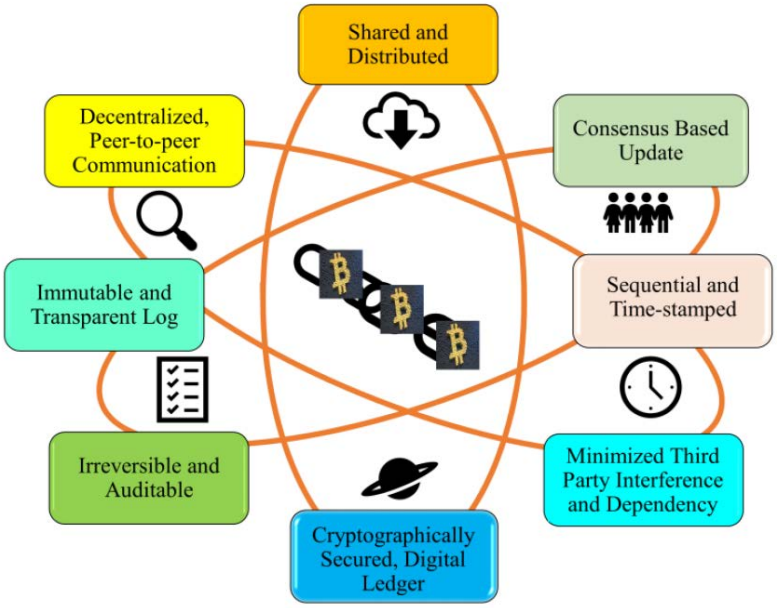

Figure 3: Blockchain characteristics [13]

Blockchain technology can be employed to solve IoT security issues. Some of the Blockchain features that are relevant for IoT security are mentioned below,

- Blockchain offers a huge address range in comparison with IPv6 whose address space is 128 bit long whereas, Blockchain has 160 bit long space. It allows, in turn, to connect billions of more devices than IP based network, making it a more viable solution for IoT as compared to IPv6 [13].
- Blockchain can be used to provide registration and identification to devices on IoT network. IoT devices have attributes, relationships, features and capabilities. Relationships comprise of device-to-device, device-to-human, device-to-service. Blockchain technology offers to solve these challenges.
- Using Blockchain technology to connect IoT devices offers the inherent advantages of security features based on cryptographic algorithms. The integrity and authentication of transmitted data is ensured when the sender and user's identity is verified and authenticated by the Blockchain network. All communication and data transactions would be recorded and tracked on the shared database called ledger.
- Blockchain networks for smart contracts provide the functionality of decentralized authentication rules and logic to authenticate an IoT device. In contrast to traditional authorization protocols, smart contracts offer less complicated authentication rules.
- Smart contract based Blockchain networks maintain data privacy by managing and controlling the users rights like right to perform software upgrade, install software patches, handle the IoT devices software or hardware related operations [12].
- IoT Communication protocols are not secure by design. Additional measures have to be taken to make IoT device communication secure which increase the computational overhead. With Blockchain networks, security protocols are simplified which become more suitable for IoT devices having limited memory and computational capacity.

The concept of using Blockchain networks for solving the security threats of IoT networks is relatively new. It is expected that this technology can benefit IoT in terms of billing, e-trading, shipping, supply chain management, asset tracking, smart metering etc [13].

7. Constraints in IoT Security

Some of the constraints and limitations in IoT security are presented in [2,4,7]. IoT architecture is resource constrained having limited memory and computing power. It is the main bottleneck in developing a robust security mechanism. Cryptographic algorithms have to be implemented within these constraints. Implementation of new security and communication protocols requires increased storage and energy requirements. It implies that these protocols must be adapted to be less compute intensive and energy efficient [11]. Other constraints include updating and managing software of devices in IoT network, device ownership, data privacy. Moreover, Blockchain technology based solutions introduce vulnerabilities of this technology in IoT networks like scalability, efficiency, hacking attacks, privacy of transactions and standardization problems [14].

8. Recommendations

IoT networks are heterogeneous in nature. It, therefore, requires the security framework to be multilayered and adaptable to IoT architecture that can dynamically select the security mechanism at different layers. In order to develop a comprehensive security scheme for IoT networks, the security protocols at multiple layers must be made interoperable by deploying conversion algorithms. It is important to develop standards and mechanisms to guarantee adequate availability of devices in IoT networks, add redundancy to network in case of single point of failure and maintain balance between cost and reliability of entire network. Embedded devices in IoT network are resource limited and are open to hardware malfunctioning. Security schemes, routing algorithms, packet processing algorithms, verification and validation protocols are required to be developed to prevent security problems at hardware level.

9. Conclusion

The present status of IoT networks poses serious challenges in terms of limited hardware resources, immature standards, security issues at hardware and software level. The diversity of IoT network is a major bottleneck to develop a universal security protocol compatible with all IoT layers. In this article, an overview is provided on IoT security challenges, attacks on IoT network, their classification into low, mid and high level issues and the corresponding solutions. Blockchain technology based solutions are also reviewed. Open challenges to IoT research community are also highlighted in order to develop stable, reliable and efficient solutions to IoT network security.

References

[1] International Telecommunication Union, “Measuring the Information Society Report,” International Telecommunication Union (ITU), Report, 2015.

[2] Minhaj Ahmad Khan , Khaled Salah, “ IoT security: Review, blockchain solutions, and open

challenges, Future Generation Computer Systems", Future Generation Computer Systems 82 (2018) 395–411.

[3] G. Noubir, G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures", SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[4] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone", Trans. Info. for.Sec. 9 (10) (2014) 1617–1628.

[5] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches", IEEE Signal Process. Mag. 30 (5) (2013) 29–40.

[6] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, "Channel-Based detection of sybil attacks in wireless networks", IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.

[7] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V.C.M. Leung, Y.L. Guan, "Wireless energy harvesting for the Internet of Things", IEEE Commun. Mag. 53 (6) (2015) 102–108.

[8] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things", IEEE Access 4 (2016) 2292–2303.

[9] A.M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Crypto-Currencies", first ed., O'Reilly Media, Inc., 2014.

[10] J. Mattila, "The blockchain phenomenon: The disruptive potential of distributed consensu architectures", ETLA working papers: Elinkeinoelämän Tutkimuslaitos, Research Institute of the Finnish Economy, 2016.

[11] H. Kim, "Protection against packet fragmentation attacks at 6LoWPAN adaptation layer", International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801.

[12] Mazonka, Oleg, "Blockchain: Simple Explanation", Journal of Reference, 29 December 2016.

[13] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems", IEEE Consumer Electronics Magazine, Volume 7, Issue 4, July 2018, pp. 06-14.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", Proceedings of the IEEE International Congress on Big Data, pp. 557-564, 2017.

[15] C.H. Liu, B. Yang, T. Liu, "Efficient naming, addressing and profile services in Internet-of-Things sensory environments", Ad Hoc Netw. 18 (Suppl. C) (2014) 85–101.