Review on Internet of Things (IoT) Security

Neeraj Kumari
College of Computing Sciences and IT,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT: With the advent of smart homes, smart cities, and smart everything, the Internet of Things (IoT) has emerged as an area of incredible impact, potential, and growth, with Cisco Inc. predicting to have 50 billion connected devices by 2020. However, most of these IoT devices are easy to hack and compromise. Typically, these IoT devices are limited in compute, storage, and network capacity, and therefore they are more vulnerable to attacks than other endpoint devices such as smartphones, tablets, or computers. In this paper, we present and survey major security issues for IoT. We review and categorize popular security issues with regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management. We outline security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions. Furthermore, we tabulate and map IoT security problems against existing solutions found in the literature. More importantly, we discuss, how blockchain, which is the underlying technology for bitcoin, can be a key enabler to solve many IoT security problems. The paper also identifies open research problems and challenges for IoT security

KEYWORDS: Blockchain, Data security, IoT security, IoT protocols, Network security.

INTRODUCTION

With the rapid growth of smart devices and high speed networks, the Internet of Things (IoT) has gained wide acceptance and popularity as the main standard for low-power lossy networks (LLNs) having constrained resources. It represents a network where ‘‘things’’ or embedded devices having sensors are interconnected through a private or a public network. The devices in IoT can be controlled remotely to perform the desired functionality. The information sharing among the devices then takes place through the network which employs the standard protocols of communication. The smart connected devices or ‘‘things’’ range from simple wearable accessories to large machines, each containing sensor chips. For instance, the Lenovo smart shoes contain chips which provide support of tracking and analyzing fitness data. Similarly, the electrical appliances including washing machines, and refrigerators can be controlled remotely through IoT. The security cameras installed for surveillance of a location can be monitored remotely anywhere in the world.

The Internet of Things (IoT) has achieved widespread adoption with the exponential development of smart devices and high-speed networks popularity and resource limitations as the principal norm of low-power failure networks. It is a network of "things" or embedded devices with sensors related by a private or public network. The IoT systems may be centrally operated for the intended purpose of the feature[1]. The exchange of information between the systems and the network that uses the standard communication protocols takes place. The intelligent linked devices or "things" span from basic wearable to massive computers, sensor chips included. Lenovo smart sneakers, for example contain chips that support exercise data monitoring and analysis. IoT meets the community's interests in addition to personal use. Good. Different intelligent devices that provide various features such as hospital surveillance, weather detection, vehicle monitoring and connectivity, and animal recognition with biochips are now serving specific interests of the society[2].

This data was collected in order to increase the performance of the systems in real time as a whole due to its implementation, the potential relevance of IoT is obvious every day. It keeps rising fast because of the success of techniques such as bandwidth enhancement by the integration of cognitive radio networks to counter the underuse of frequency spectrum. Hardware techniques. The literature has now grown into integral components of Wireless Sensor Networks (WSN), machine-to-machine (M2M) and cyber physical systems (CPS) for the larger IoT word. The safety issues hence in conjunction with WSN, M2M or CPS, in connection with the key standard for networking is the IoT with the IP protocol.

Therefore, the whole operating architecture must be protected attacks that could also impede the IoT resources as a challenge to data protection, completeness or privacy. Since IoT depicts an integrated set it inherits traditional networks and heterogeneous devices Computer network security challenges. The restriction resources face additional IoT security challenges because the tiny sensors or things have minimal memory and power. The protection solutions must also be tailored to the architectures limited. The remainder of the document is structured accordingly. A summarizes the IoT architecture and the security problems stack protocol implemented by IoT on any layer[3]. The key safety problems are classified, while Section 4 analyses and a mapping of the possible solutions is defined. Specific block chain protection strategies are discussed and evaluated addresses the problems raised by study key challenges to IoT security and its potential solutions ends the paper.

DISCUSSION

Iot Architecture and Security Challenges:

A standard IoT implementation involves heterogeneous appliances the IoT systems are special and are often integrated with network-connected sensors. Low capacity, minimal memory and limited processing characteristics Capability. The gates are used for linking IoT to external environments to provide IoT users with remote data and facilities. Represents a typical IoT layered architecture device & Communications protocols, routing/forwarding, Physical and key control systems and security devices. It incorporates the widely used specifications and protocols low-rate LR-WPAN and the broadband networks low-power wide-area network protocols recently built protocols (LPWAN)[4]. The IEEE 802.15.4 defines two low-level layers for LR-WPANs: the physical layer and the medium access control (MAC) Layer. The contact is connected to the physical layer specification across radio networks of different bands and details of frequency tariffs. Mechanisms for the MAC layer specification access to all channels and sync. Since the scale is limited to a full unit (MTU) of transmission used by IEEE 802.15.4 IPv6 over low-performance wireless networks for the personal area. The adaptation layer (6LoWPAN) above the connection layer is incorporated to boost IP-based connectivity sensor node Functions each IoT system is special to an IPv6.

Address of the network. The Low Power and Failure Routing Protocol the 6LoWPAN ecosystems support networks (RPL) are used. The RPL norm serves all point-to-point traffic and multi-point contact and single point communication the LPWAN offers a wide selection of "things" in IoT. In comparison to a WAN that needs more strength it facilitates low-power communication with low bit rate in order to operate at a high bit rate. For the LPWAN the protocol LoRa WAN is used to connect between gateways and terminals when promoting differing data rates in a battery-operated network. Likewise, a 3GPP Protocol for Narrow-Band IoT (NB-IoT) LPWANs contact for indoor coverage during use of spectrum in LTE. In unidirectional, bidirectional and low-power modes the Wigless protocol uses three separate communication specifications in the LPWAN.

1. Data Privacy, Confidentiality and Integrity

As IoT data flows in a network across a number of hops, mechanisms of encryption are important to ensure secrecy of info. - Data. Since operation, devices and network integration is complex, device-specific data is subject to breach of privacy compromise nodes in an IoT network. compromise. IoT appliances an attack-prone assailant can have an effect on the data integrity by modification of stored records for malicious purposes[5].

2. Authentication, Authorization and Accounting:

Authentication is essential to secure communication in IoT communicating with one another between two sides. Apps must be authenticated for privileged access to facilities. There are primarily due a variety of IoT authentication mechanisms to the complex heterogeneous underlying IoT interface supporting architectures and ecosystems. These contexts are a challenge to define the world standard authentication protocol in IoT. The authorization processes often ensure that the authorized parties have access to networks or information. An appropriate authorization and authentication results in a reliable system that promises a safe environment to correspond. For communication. In addition, capital utilization accounting, audit and monitoring together provide a consistent process to protect the maintenance of the network.

3. Availability of Services:

Assaults on IoT devices can impede service delivery. Conventional assaults for denial of service. Different tactics, like sinkholes, jamming opponents or the replay attacks use IoT components at multiple layers to change IoT users' level of service.

4. Energy Efficiency:

IoT systems are normally space limited and have low power and less capacity. The IoT strikes architectures can contribute to increased consumption of energy flooded the network and exhausted IoT services redundant or forged orders for service

Categorization of Security Issues:

The IoT paradigm requires a wide range of gadgets and equipment varying between small and large embedded chips high-end servers, it would fix security vulnerabilities. A taxonomy of IoT vulnerability problems references relevant to the publishing of each issue. We identify threats to protection about IoT architecture implementation

As illustrated below.

- Low-level security issues
- Intermediate-level security issues
- High-level security issues

Block Chain Solutions for IoT Security:

The industry and the academic community has foreseen Block chain technology as an awkward technology that plays an important role in administration, control and above all IoT devices to safety. This segment discusses how block chain can be done as a crucial technology that allows sustainable security solutions to today's IoT security issues to be provided. The first part provides a short history and then outlines open Block chain IoT technology considerations of analysis and block chain threats for solutions may have. This segment also discusses the literature of IoT protection issues block chain-based implementations.

CONCLUSION

IoT systems are currently unstable and unable to protect their own. This is primarily because of the limited IoT capital the lack of protected hardware, devices and immature requirements plan, development and implementation of applications. The commitment of defining a comprehensive global IoT layer protecting process and the diversity of IoT tools is also hindered. We discuss and examine the key IoT security problems in this document. We identify those questions depend on the intermediate stage, at high level, and IoT layers of low-level. We chat briefly about the arrangements suggested in the literature to make use of IoT protection ebenen. Parametric study of and potential IoT attacks there are also options. We look at the effect of the attack and map them in the literature with potential solutions. We also explore how to answer and use the block chain to solve some of the security challenges most important to IoT. The text outlines and discusses future and open problems in research and challenges which the research group must resolve to ensure IoT security that is consistent, effective and scalable solutions

REFERENCES

[1] R. H. Weber, "Internet of Things - New security and privacy challenges," *Computer Law and Security Review*, 2010, doi: 10.1016/j.clsr.2009.11.008.

[2] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," 2016, doi: 10.1109/HICSS.2016.714.

[3] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Computer Networks*. 2017, doi: 10.1016/j.comnet.2016.11.007.

[4] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," *Computer Law and Security Review*, 2016, doi: 10.1016/j.clsr.2015.12.001.

[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," 2012, doi: 10.1109/ICCSEE.2012.373.