A Review on Block Chain Solutions and Open Problems in IoT Security

Paras Nath Mishra, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id-paras.m@arkajainuniversity.ac.in

ABSTRACT: ***With the introduction of smart homes, smart cities, and smart everything, the Internet of Things (IoT) has emerged as a sector with enormous promise, with Cisco Inc. projecting 50 billion linked devices by 2020. The majority of these IoT gadgets, on the other hand, are simple to hack and infiltrate. These IoT devices often have lower computing, storage, and network capacities, making them more susceptible to attacks than other endpoint devices like smart phones, tablets, or PCs.We discuss and review key security concerns for IoT in this article. We examine and classify common security concerns in relation to the IoT layered architecture, as well as networking, communication, and management protocols. We discuss IoT security needs, as well as current attacks, threats, and cutting-edge solutions. In addition, we compile a list of IoT security issues and link them to current solutions in the literature. More significantly, we explain how blockchain, the underlying technology underpinning bit coin, may be used to address a variety of IoT security issues. In addition, the report highlights outstanding research issues and difficulties in the field of IoT security.***

KEYWORDS: Block Chain, Data, IoT Security, IoT Protocols, Network, Security.

1. INTRODUCTION

The Internet of Things (IoT) has achieved broad recognition and appeal as the primary standard for low-power lossy networks (LLNs) with limited resources, thanks to the fast development of smart gadgets and high-speed networks. It is a network in which ‘‘things," or embedded devices with sensors, are linked through a private or public network. The gadgets in the Internet of Things (IoT) may be operated remotely to fulfill the required purpose. The information is subsequently shared across the devices through the network, which uses industry-standard communication protocols. The smart linked devices, or ‘‘things," include anything from small wearables to huge machinery, all of which include sensor chips. Take, for example, the Lenovo smart sneakers. Corresponding author' is a term that refers to a person who include chips that assist with the monitoring and analysis of fitness data. Electrical equipment, such as washing machines and refrigerators, may also be operated remotely via IoT. The security cameras that have been placed to monitor a site may be seen remotely from anywhere in the globe. Apart from personal usage, IoT also serves the requirements of the society. Various smart gadgets that perform various functions such as monitoring operations in hospitals, sensing weather conditions, providing tracking and connection in cars, and animal identification utilizing biochips are already fulfilling community requirements.

The data gathered by these sensors may be analyzed in real time to enhance the overall system's efficiency. The use of IoT in daily life demonstrates its future importance. It is still growing quickly due to advancements in hardware methods such as increasing bandwidth by integrating cognitive radio-based networks to solve underutilization. Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) or Cyber Physical Systems (CPS) have now developed as essential components for the larger term Internet of Things (IoT) in the literature. As a result, security issues connected to WSN, M2M, and CPS continue to emerge in the context of IoT, with the IP protocol serving as the primary connection standard. As a result, the whole deployment architecture must be protected against threats that may obstruct IoT services or jeopardize data privacy, integrity, or confidentiality.Because the Internet of Things is made up of linked networks and diverse devices, it inherits the security problems that plague computer networks. Because tiny devices or objects with sensors have limited power and memory, IoT security is further complicated by resource constraints. As a result, security solutions must be tailored to the limited architectures [1].

In recent years, a lot of work has gone into dealing with security concerns in the IoT paradigm. Some of these methods focus on a particular layer of security, while others seek to provide end-to-end security for IoT. Security problems are classified in provides a review of privacy-preserving IoT methods. The author explains

how to implement safe multi-party calculations to protect IoT users' privacy. Credit checking and attribute-based access control are presented as viable methods for protecting privacy in the Internet of Things [2]. For cloud-based IoT, Zhou et al. address several security risks and potential solutions. Identity and location privacy, node compromise, layer removal or addition, and key management risks for IoT utilizing clouds are all described by the authors. Address key IoT security problems such as unique item identification, authentication and authorization, privacy, the necessity for lightweight cryptographic methods, malware, and software vulnerabilities in another study. The IOT-a project outlines an IoT reference architecture that must be implemented in order to provide trust, privacy, and security. Through an authentication method, the trust model is intended to guarantee data integrity and secrecy while allowing end-to-end communication. Furthermore, the privacy model necessitates establishing access rules and methods for encrypting and decrypting data in order to prevent inappropriate data use.

The security component is divided into three layers: services, communications, and applications. The Open Web Application Security Project (OWASP) also lists the top ten vulnerabilities for IoT design. Unsecured interfaces of IoT architectural entities, improper security setup, physical security, and insecure software/firmware are among the risks. A parametric study of security risks and how they relate to IoT solutions.Taxonomy and classification of IoT security problems based on its layers, as well as the countermeasures employed to solve them. A discussion of the fundamental features of blockchain-based security solutions, as well as an assessment of their efficacy in safeguarding IoT. Future prospects, emphasizing potential solutions to open IoT security issues. The remainder of the paper is laid out as follows. The IoT architecture and security issues encountered at each tier of the protocol stack used by IoT are described in classifies the major security concerns, while Section 4 examines and provides a mapping of the suggested remedies., we address the research problems presenting the most significant impediment to IoT security and their potentialremedies.Security and IoT Architecture ChallengesA typical IoT deployment consists of heterogeneous devices with integrated sensors that are linked through a network. IoT devices are easily distinguished by their low power consumption, tiny memory, and limited computing capacity. The gateways are used to link IoT devices to the outside world so that data and services may be delivered to IoT consumers remotely [3].

2. DISCUSSION

A layered architecture that includes standard IoT protocols for applications and messages, routing and forwarding, physical devices, and key management and authentication. It contains the standards and protocols for the most widely used technologies.LR-WPANs (low-rate wireless personal area networks) [24], and Protocols for low-power wide-area networks have recently developed. Protocols based on the Low Power Wide Area Network (LPWAN). The IEEE standard 802.15.4 defines two low-level layers for LR-WPANs: the Physical Layer and the Medium Access Control Layer (MAC) layer. The communication layer standard is linked to the physical layer definition across a network of wireless channels with a variety of frequency bands and data rates. The MAC layer standard is concerned with methods for transferring data between computers. Access to the channel as well as synchronization Because of its tiny size, in order to provide IP-based connectivity to sensor nodes capabilities. An IPv6 address is used to identify headdress of a network The Low-Power and Lossy Routing Protocol PAN settings are supported by Networks (RPL).

The RPL standard allows both point-to-point and multi-point communication. Between many points and a single point, communication is possible. Because of the restricted payload, IoT application architecture uses User Datagram Protocol (UDP) for communication.TCP is regarded to be less efficient and complicated. Furthermore, UDP header compression may be used to improve performance. Maximizing the limited cargo space available [4]. In terms of control messages, The Internet Control Message Protocol (ICMP) is used for things like indicating inaccessible destinations and neighbor finding.6LoWPAN is a user on 6LoWPAN. The Constrained Application Protocol (CoAP) is a protocol for constrained applications offers a request–response paradigm for low-power lossy communication. In restricted settings, networks exist. The CoAP protocol is a mechanism for transferring data between computers offers asynchronous message communication as well as to access IoT resources through HTTP, use the HTTP mapping. The LPWAN enables ‘‘things" to communicate over great distances in the Internet of Things A wired WAN, on the other hand, requires greater electricity. It enables low-power communication with low bit-rate to operate with a high bit-rate. The Lora WAN protocol is used by the LPWAN.In a network of battery-operated objects, communication between gateways and end

devices must be supported while supporting variable data speeds. Similarly, narrow-band IoT (NB-IoT) is a 3GPP protocol for Internet of Things.

In LPWANs, communication is used to offer interior coverage while using The LTE spectrum The Weightless protocol supports unidirectional, bidirectional, and low-power communication modes in LPWAN using three distinct standards. Various methods and factors must be considered for a secure IoT implementation, as detailed below. Confidentiality, privacy, and integrity of data Because IoT data goes via many hops in a network, it requires special protection. To guarantee the secrecy of data, an encryption method is needed. Data. Because of the many services, devices, and networks that have been integrated, Data saved on a gadget may be subject to privacy violations. In an IoT network, compromising nodes is possible. The Internet of Things (IoT) device As a result of being vulnerable to attacks, an attacker may have an effect on the data [5]. Integrity by tampering with the data saved for nefarious reasons Authentication, authorization, and accounting Authentication is needed for IoT connection to be secure between two parties that are in communication with one another. The devices must be authenticated in order to have privileged access to services.

The Because of this, there is a wide range of authentication methods for IoT IoT devices are supported by a variety of heterogeneous underlying architectures and ecosystems. These situations are dangerous. Defining a uniform worldwide authentication protocol is a difficult task. in the Internet of Things Similarly, permission procedures guarantee that only those who are authorized have access to systems or information [6]. Appropriate authorization and authentication results implementation in a dependable atmosphere that guarantees a safe environment for the purpose of communication Furthermore, resource use accounting, offer a trustworthy method in addition to auditing and reporting for network management security Attacks on IoT devices may make it difficult to provide services.via traditional denial-of-service (Do) assaults Sinkhole assaults, jamming opponents, and other tactics are among the options.

Replay attacks take use of IoT components at several levels to degrade the quality of service (QoS) delivered to IoT consumers. Energy conservation IoT devices are generally resource restricted, with minimal power consumption and limited storage. Attacks against the Internet of Things Energy consumption may rise as a consequence of new designs by overburdening the network and depleting IoT resources service requests that are duplicated or falsified Faults with a single point of failure The continual development of heterogeneous networks for IoT-based infrastructure may expose a significant number of single-points-of-failure, causing the services to degrade.via the Internet of Things It requires the creation of a tamper-proof system to offer a fault-tolerant environment for a large number of IoT devices as well as various methods for implementing a fault-tolerant.

2.1. Application:

Unsafe discovery of a neighbor. Every device on the network must be individually identifiable according to the IoT deployment architecture. To guarantee that the data being sent to a device in end-to-end communication reaches the designated destination, the message transmission used for identification must be secure. Prior to data transmission, the neighbor discovery phase performs a number of tasks, including router detection and address resolution. The use of neighbor discovery packets without appropriate verification may result in serious consequences, including denial of service. Attack with a reservation buffer. An attacker may take advantage of this by delivering incomplete packets to a receiving node, which needs buffer space for reassembling incoming packets. Due to the space filled by the attacker's unfinished packets, additional fragment packets are rejected, resulting in a denial-of-service attack. Routing attack using RPL. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is susceptible to a number of attacks that are initiated by hacked network nodes.

The assault may result in resource loss and eavesdropping. Attacks from sinkholes and wormholes Sinkhole attacks occur when an attacker node replies to routing requests, causing packets to route via the attacker node, which may then be exploited to conduct malicious network activities. Wormhole attacks, in which a tunnel is constructed between two nodes such that packets arriving at one node reach the other node instantly, may further degrade 6LoWPAN operations. Eavesdropping, privacy violations, and denial-of-service assaults are all possible outcomes of these attacks. Sybil wreaks havoc on the intermediary levels. Sybil nodes, like Sybil attacks on low-level layers, may be used to impair network speed and potentially compromise data privacy. Authentication and Integrity of Data sent by IoT devices linked to the blockchain network is always

cryptographically proofed and signed by the actual sender, who has a unique public key and GUID, guaranteeing authenticity and integrity. Furthermore, all transactions performed to or by an IoT device are recorded on the blockchain global ledger and can be securely monitored [7].

Authentication, Authorization, and Privacy are the three pillars of security. Smart contracts on the blockchain can give decentralized authentication rules and logic to an IoT device, allowing for single and multiparty authentication. When compared to conventional authorization protocols like Role Based Access Management (RBAC), Oaths 2.0, OpenID, OMA DM, and LWM2M, smart contracts may offer more effective authorization access rules to connected IoT devices with much less complexity. These protocols are often used to authenticate, authorize, and manage IoT devices these days. Furthermore, data privacy may be maintained via the use of smart contracts, which define the access rules, circumstances, and timeframes that enable a specific person or group of users or machines to own, manage, or access data in transit or at rest. Smart contracts may also specify who has the authority to update, upgrade, patch, or reset IoT software or hardware, provide new key pairs, start a service or repair request, change ownership, and provision or re-provision the device.

Communication that is secure. By design, IoT application communication protocols like HTTP, MQTT, CoAP, or XMPP, as well as routing protocols like RPL and 6LoWPAN, are not secure. To enable secure communication, such protocols must be wrapped inside other security protocols such as DTLS or TLS for message and application protocols. IPSec is also often used to offer security for RPL and 6LoWPAN protocols in routing. In terms of compute and memory needs, DTLS, TLS, IPSec, and even the light-weight TinyTLS protocols are heavy and complex, and compounded by a centralized administration and governance of key management and distributes utilizing the popular PKI protocol. Key management and distribution are completely removed with blockchain since each IoT device will have its own unique GUID and asymmetric key pair once linked to the blockchain network. Other security protocols, such as DTLS, will be significantly simplified as a result of this, as there will be no need to handle and exchange PKI certificates during the handshake phase of DTLS or TLS (or IKE in the case of IPSec) to negotiate the cipher suite parameters for encryption and hashing, as well as to establish the master and session keys. As a result, light-weight security methods that suit and stratify the needs of IoT devices' computation and memory resources become increasingly viable[8].

2.2. Advantages:

Authentication and secure communication. The devices and users in IoT need to be authenticated through key management systems. Any loophole in security at network layer or large overhead of securing communication may expose the network to a large number of vulnerabilities. For instance, due to constrained resources, the overhead of Datagram Transport Level Security (DTLS) requires to be minimized, and the cryptographic mechanisms ensuring secure communication of data in IoT must take into account the efficiency as well as the scarcity of other resources. Transport level end-to-end security. The transport level end to-end security aims at providing secure mechanism so that the data from the sender node is received by the desired destination node in a reliable manner. It requires comprehensive authentication mechanisms which ensure secure message communication in encrypted form without violating privacy while working with minimum overhead. An attacking node can impersonate the victim node to continue the session between two nodes. The communicating nodes may even require re-transmission of messages by altering the sequence numbers. Privacy violation on cloud-based IoT Different attacks which may violate identity and location privacy may be launched on cloud or delay tolerant network based IoT.

Similarly, a malicious cloud service provider on which IoT deployment is based, can access confidential information being transmitted to a desired destination. High-level security issues the high-level security issues are mainly concerned with the applications executing on IoT as described below. CoAP security with internet. The high-level layer containing the application layer is also vulnerable to attacks. The Constrained Application Protocol (CoAP) being a web transfer protocol for constrained device uses DTLS bindings with various security modes to provide end-to-end security. The CoAP messages follow a specific format defined in RFC-7252, which need to be encrypted for secure communication. Similarly, the multicast support in CoAP requires adequate key management and authentication mechanisms. Insecure interfaces. For accessing IoT services, the interfaces used through web, mobile, and cloud are vulnerable to different attacks which may severely affect the data privacy. Insecure software/firmware. Various vulnerabilities in IoT include those caused by insecure

software/firmware. The code with languages such as JSON, XML, SQLi and XSS needs to be tested carefully. Similarly, the software/firmware updates need to be carried out in a secure manner. Middleware security. The IoT middleware designed to render communication among heterogeneous entities of the IoT paradigm must be secure enough for provision of services. Different interfaces and environments using middleware need to be incorporated to provide secure communication [9] .

2.3. Working:

The security header and use mode are described by the first three bits of the dispatch type values, while the remaining three bits specify the kinds of 6LoWPAN addressing headers. A 2-byte Security Parameters Index (SPI) is used to retrieve information from a packet about the cryptographic methods and keys that will be used to process the packet.] offer a protocol for protecting IoT against denial-of-service (Do's), man-in-the-middle, and replay attacks, which is in opposition to this method. Attackers may send messages for resource usage on limited devices, resulting in Do's attacks. In a networked setting, the secret keys disclosed by eavesdropping may result in identity theft due to main-in-the-middle attacks. Furthermore, attackers may repeat identifying information or credentials to disrupt network traffic. The suggested Identity Authentication and Capability based Access Control (IACAC) method produces secret keys using the Daffier Hellman algorithm based on Elliptic Curve Cryptography. The devices are mutually authenticated for communication and access via encryption and secret keys.The capability represents a structure comprising access permissions and the device identification, and the capability is used to perform capability-based access control.

The communication between two devices is first confirmed when using capability-based access. Furthermore, the device's capacity to execute the required functionality is verified prior to the actual operation. Kothmayr et al. propose a two-way authentication method based on public key cryptography for end-to-end security. The network's publishers' access permissions are stored on a trustworthy Access Control server. The publisher's certificate and the Certificate Authority (CA) must both be present on the publisher's website.The authentication may be done using RSA or DTLS pre-shared keys utilizing the Trusted Platform Module (TPM) chips. The RSA certificates are sent in X.509 format using TPMs. End-to-end communication is only allowed once subscribers have been authenticated by the Access Control server.The suggested method has been shown to operate with minimal energy and memory needs. Huang et al. offer another authentication and authorization method based on several factors. When utilizing smart cards, the suggested method includes password authentication. The secret random string is then extracted from biometrics using a fuzzy extractor. The authentication protocol allows for the establishment of security settings, the storage of registration information in a database, authentication, and the change of authentication credentials, among other things [10]. The authors also provide a stand-alone authentication method in cases when the authentication server is unavailable.

3. CONCLUSION

IoT devices nowadays are unsafe and unable to protect themselves. This is due to a lack of secure hardware and software design, development, and deployment in IoT devices, as well as limited resources in IoT devices, immature standards, and the lack of secure hardware and software design, development, and deployment. Due to the variety of resources in IoT, attempts to define a strong global method for protecting the IoT layers are further hindered. We examine and discuss key IoT security concerns in this article. We divide these problems into three categories: high-level, intermediate-level, and low-level IoT layers. We review the methods proposed in the literature for exploiting IoT security at various levels in a concise manner. In addition, a parametric study of IoT attacks and potential remedies is given. We examine the ramifications of the assault and connect them to potential remedies suggested in the literature. We also go through how blockchain technology may be utilized to address and solve some of the most pressing IoT security issues. In order to offer reliable, efficient, and scalable IoT security solutions, the article also describes and identifies future and open research problems and difficulties that must be addressed by the research community.

REFERANCES

[1] X. Wu, X. Zhu, G. Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, 2014.

[2] W. Xu *et al.*, "Internet of vehicles in big data era," *IEEE/CAA J. Autom. Sin.*, 2018.

[3] J. Bughin, "Big data, Big bang?," *J. Big Data*, 2016.

[4] L. N. Sanchez-Pinto, Y. Luo, and M. M. Churpek, "Big Data and Data Science in Critical Care," *Chest*. 2018.

[5] R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*. 2017.

[6] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors (Switzerland)*. 2018.

[7] R. Dou and G. Nan, "Optimizing sensor network coverage and regional connectivity in industrial IoT systems," *IEEE Syst. J.*, 2017.

[8] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, 2018.

[9] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, 2018.

[10] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, 2018.