International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2498-2500 www.ijaem.net ISSN: 2395-5252

IoT Security: Ongoing Challenges and Research Opportunities

Darshan, Rajiv, Rahul

Student ,M.Tech , Dept. of Computer Science , Shri Baba Mastnath College of Engineering & Technology Rohtak , Haryana , India
Asst. Prof. , Dept. of Computer Science , Shri Baba Mastnath College of Engineering & Technology Rohtak , Haryana , India
Asst. Prof. , Dept. of Computer Science , Shri Baba Mastnath College of Engineering & Technology Rohtak , Haryana , India

Submitted: 05-07-2021 Revised: 17-07-2021 Accepted: 20-07-2021

ABSTRACT: The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected. In this paper, we begin with general information security background of IoT and continue on with information security related challenges that IoT will encountered. Finally, we will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters .

I. INTRODUCTION

When the term "Internet of Things" (IoT) was first introduced, the initial question could be what is considered as "Things". Till recent years, groups of researchers and organizations tried to clarify the definition of IoT. Haller et al. [1] proposed a definition of IoT with "A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business process." To extend the coverage of IoT definition, Sarma et al. [2] defines the "Things" from physical objects to virtual objects which represents as the identities with Internet connectivity. Although IEEE IoT Initiative is proceeding to draft a white paper [3] for the formal definition of IoT there are still no common agreements for the definition of IoT. In this article, we define a "Thing" on IoT that indicates a physical or virtual object which connects to the Internet and has the ability to communicate with human users or other objects.The rapid proliferation of the Internet of Things (IoT) into diverse application areas such as building and home automation, smart transportation systems, wearable technologies for healthcare, industrial process control and infrastructure monitoring and control is changing the fundamental way in which the physical world is perceived and managed. It is estimated that there will be about 30 billion IoT devices by 2020. Most of these IoT devices are expected to be of low-cost and wireless communication technology based, with limited capabilities in terms of computation and storage. As IoT systems are increasingly being entrusted with sensing and managing highly complex eco-systems, questions about the security and reliability of the data being transmitted to and from the IoT devices are quickly becoming a major concern.

II. RELATED WORK

The term Internet stands for the holistic global networking infrastructure which scopes from private, public, academic, cooperate networks to government networks [1]. The connectivity through the Internet is formulated by Transmission Control Protocol / Internet Protocol (TCP/IP) and secured through various protocols such as Secure Socket Layer (SSL) / Transmission Layer Security (TLS), IPSec and Secure Shell (SSH). Though in IoT, Datagram Transport Layer Security (DTLS) is used as the communication protocol. Since the Internet is accessible for everyone, the amount and nature of vulnerabilities outweight the effectiveness of existing secure communication protocols due to its implosive access capacity. Probable attacks are viruses, worms, hacking, cyber bullying, identity theft, consent and Distributed DoS (DDoS). Countermeasures to overcome these attacks include Identity Management for confidentiality, Encryption schemes for confidentiality of communication channels, Cloud based solutions to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2498-2500 www.ijaem.net ISSN: 2395-5252

establish secure channels based on PKI for data and communication confidentiality.All the monitoring applications are developed with IoT infrastructure with grid controlling access granted to the grid controlling officers for pursuing configurations while the consumers could only visualize the consumption details via a mobile device. The information circulated through the AMI would pose a privacy concern for consumers for disseminating information regarding their habitual activities, where the impact could be severe for industries. Due to the heterogeneous nature of communication equipment deployed with IoT and rapidly increasing population and industries, it would cause scalability issues for security. Smart girds are distributed across the power serving area and are exposed to adversaries. As the energy distribution system is the most critical infrastructure that exists in an urban area, the conversion of the current power line communication (sending data over existing power cables) based controlling and monitoring channels to the wireless medium with the introduction of IoT technologies would expose the entire system into unintended security vulnerabilities. The intruders could perpetuate AMI interfaces stationed at every household or industrial plant with proper techniques. Once the access is granted to the hostile operators, potential outcomes could be devastating as to the level of disrupting the energy flow of a local grid substation to overloading a nuclear reactor of a power station. The availability of the grid could be compromised from IP spoofing, injection and DoS / DDoS attacks. Thus, access controlling for devices used in AMI and grid controlling system should be secured with extra countermeasures.Intelligent Transportation Systems (ITS) are introduced to improve transportation safety and degrade traffic congestions while minimizing the environmental pollution. In an ITS system, there are four main components such as vehicles, road side stations, ITS monitoring centre and security system [41]. All the information extracted from vehicular nodes and road side stations are conveyed to the ITS monitoring center for further processing, while the security subsystem is responsible for maintaining overall secureness. The entire system could be considered as a vehicular network, while the communications are established between Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) and Vehicle-to-Grid (V2G). These communication links are implemented using technologies like RFID and Dedicated Short Range Communication (DSRC) for launching a large Wireless Sensor Network (WSN). The vehicular nodes and the entire data storing and monitoring infrastructure form a viable IoT deployment.

III. DISCUSSION

Authentication for IoT is a paramount necessity for securing and ensuring privacy of users, simply due to the fact that an impregnable access control scheme would be impervious for any attack vector originating outside of the considered trust domain, as explained in the previous sections of this book chapter. Authentication schemes in IoT applications are generally implemented in the software level, in which it exposes the hardware and design vulnerabilities that are unintentional [84]. This fact constitutes the requirement of a holistic approach for securing access to the systems via employing impregnable authentication schemes. However, developing a generic authentication scheme to counter all possible attack scenarios would be improbable and an arduous attempt due to the heterogeneity of the IoT paradigm. A layered approach which concatenates the optimum authentication schemes applicable at differentiated levels to formalize a holistic trust domain is a desideratum. For perception level entities, IBE or ECC would be ideal authentication schemes to generate commendable cryptographic credentials with available resources. The mobile entities, where the actual users are interfacing to IoT systems are storing personalized credentials such as photos, medical stats, access to CCTV systems, GPS location (GPS), daily routines, financial stats, banking credentials, emergency service status and online account statistics, are emphasizing the requisite for privacy preservation at this level. As proposed in section 3.3.2.1, adopting IBE, ABE, ECC or biometric based mechanisms should be ensuring security. Novel mechanisms such as CapBAC could be employed to launch a scalable access control scheme for cloud computing platforms for IoT applications. However, potential for deploying edge computing paradigms in the edge of the network indemnifies the cloud computing services from external direct access, as the access controlling would be migrated to the edge along with the service platform. The internet technologies of IoT enabled systems are secured than the perception level and mobile level entities with the deployed protocols such as DTLS, SSL and IPSec. Due to the dependency of a CA or TTP for employing such strong and secure protocols, the future of Internet security enhancements would be focused on developing distributed access control schemes to eliminate the single point of failure. Each IoT application composes different devices and systems to

accomplish the intended outcome which attributes diverse protocols in hardware and software. Thus, the authentication schemes should be application specific and context aware of resource constraints associated with the diversified deployments. As the privacy is the main concern on IoT to be ensured through impregnable access control schemes, the GDPR initiative is a timely solution established to constrict the IoT service providers (both software and hardware) from developed and marketing products with vulnerabilities. Current researches have focused on developing novel methods for authentication in IoT domain. We are briefly introducing few of these recent approaches to demonstrate the state of the art technologies. In , Ning et al. has proposed an aggregated proof based hierarchical authentication (APHA) scheme to be deployed on existing Unit IoT and Ubiquitous IoT (U2IoT) architecture. Their scheme employs two cryptographic primitives; homomorphic functions and Chebyshev polynomials. The proposed scheme has been verified formally using Burrows-Abadi-Needham (BAN) logic. However, the scalability of the scheme with the extent of multiple units has not been verified with a physical prototype. There are various initiatives on Physical Unclonable Functions (PUF) to be used for IoT device authentication. A PUF is an expression of an inherent and unclonable instance-specific unique feature of a physical object which serves as a biometric for non-human entities, such as IoT devices . Hao et al. are proposing a Physical Layer (PHY) End to End (E2E) authentication scheme which generates an IBE based PHY-ID which acts as a PUF with unclonable PHY features RF Carrier Frequency Offset (CFO) and In-phase/Quadrature-phase Imbalance (IQI) extracted from collaborative nodes in a Device to Device (D2D) IoT deployment. This mechanism is ideal for perception level nodes to be impervious to impersonation or malicious node injection attacks, as it is using physical measurements which are unique for each entity and for its location of operation in generating an identity for devices. Though, the proposed scheme relies on a TTP called Key Generation Centre (KGC). KGC generates the asymmetric key credentials for the nodes in its contact. The reachability of a certain KGC is limited due to the low power D2D connectivity. Thus, multiple KGCs deployed to accomplish the coverage should be managed with a centralized control entity. This enables the attack vectors on decentralized KGC entities. Moreover, the reliance on CFO and IQI features require the nodes to be stationary. This would be an issue considering most IoT devices are mobile and their RF based characteristics are varying in a timely manner. Aman et al. proposed a PUF based authentication protocol for scenarios when an IoT device is connecting with a server and a D2D connectivity focused on its applicability in vehicular networks. Authentication is based on a Challenge Response Pair (CRP), where the outcome of the CRP is correlated with the physical microscopic structure of the IoT device, which emphasizes its unique PUF attributes with the inherent variability of the fabrication process in Integrated Circuits (ICs). The proposed protocol was analysed using Mao and Boyd logic, while Finite State Machine (FSM) and reachability analysis techniques have been adopted for formal verification. Even though the performance of the protocol has been analysed in terms of computational complexity, communication overhead and storage requirement, its scalability with simultaneous multiple IoT device connections to the server have not been addressed. However, this approach would be a feasible solution for V2E applications as the PUF could be successfully integrated with vehicles.

IV. CONCLUSION

IoT technology is the most discussed paradigm in the research community these days. Its potential to connect all the devices in the world and to create a large information system that would offer services to improve the quality of human beings exponentially has made the concept much popular. The integration of various technologies and devices with different architectures are creating interoperability issues with the components in the IoT architecture. These issues and the highly diversified types of services are creating security concerns which disperse into all three layer of IoT architecture: Perception, Network and Application. Hence, the security measures to be taken should be developed while analysing the threats and vulnerabilities at each layer. Mitigating risks associated with security breaches are possible, if security receives consideration from early product planning and design, and if some basic prevention mechanisms are in place. Enactment and standardization will simplify the manufacturing and development processes, give the market an incentive for mass-adoption and also increase the security posture of IoT products and services. Security will have to be inbuilt so that IoT can withstand a chance against the threats that technological advancements will bring along.