Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue I, Jan-June 2024

REVIEW OF INVISIBLE BARRIERS: SECURITY AND PRIVACY RISKS IN IoT APPLICATIONS

Mahima Vyas[1], Kashish Vijay[2], Vishal Saxena[3], Pradeep Kumar Sharma[4], S. K. Dixit[5]
[3]E-mail: vishalsaxena.math@jecrc.ac.in

ABSTRACT:

Internet of things (IoT) is an interconnected wireless network where smart nodes (IoT devices) interact with each other in order to exchange data through the communicating medium. The Internet of things (IoT) and other contemporary ideas promise to improve quality of life, better business potential, economic production, and effective management of operation through universal connection and the introduction intelligent physical items. IoT networks are capable of collecting, pre-processing and transmitting massive amounts of data. IoT opened doors for better communication for people. But the attacker opened doors of attacks to IoT systems to make use of user's sensitive information. Given that these networks deal with real word part of our lives as well as critical infrastructure, cyber security in such networks is critical. This study delves into the critical security and privacy concerns that arise within the Application layer of IoT systems. We systematically review and categorize the prevalent threats, including data breaches, unauthorized access, and privacy invansion, highlighting how these vulnerabilities can be exploited by malicious actors.

Keywords- Internet of things (IoT), Application layer, Security concern, Privacy concern, Universal connections, Data Breaches

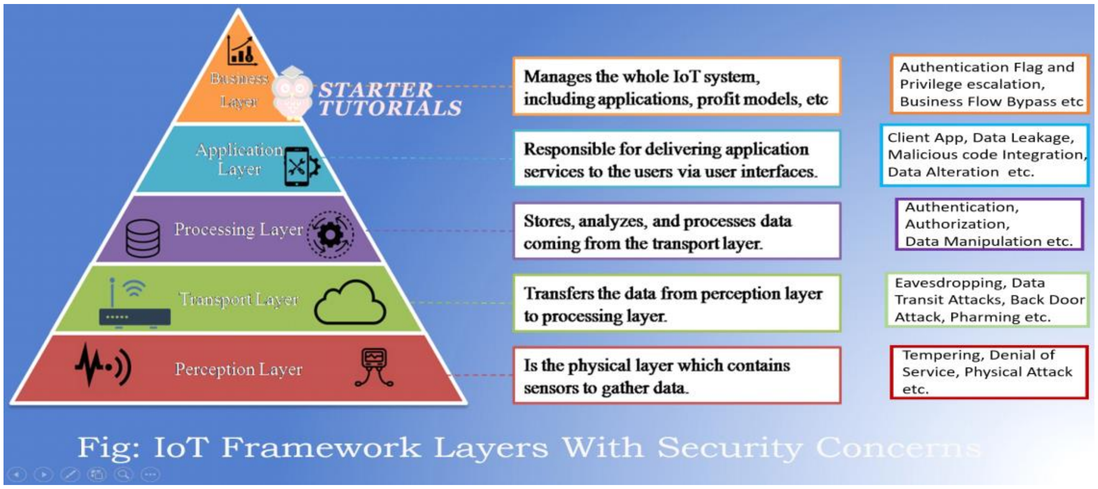
[1] INTRODUCTION

The Internet of things (IoT) represents a revolutionary paradigm in the field of computing and networking. It involves the interconnection of everyday objects equipped with sensors, software, and other technologies to communicate and exchange data over the internet. The fundamental idea behind this concept is that there are many different things all around us including sensors, mobile phones, Radio-Frequency Identification (RFID) tags, actuators etc., which are able to communicate with one another and work together with their neighbors to accomplish shared objectives. IoT garnered significant attention in recent years. Originally proposed by kevin ashton in 1999, the technology has since evolved dramatically. Advancement in Wireless Sensor Network (WSN), Radio Frequency Identification (RFID), and cloud computing have made communication between IoT devices more seamless than ever before. The IoT ecosystem includes a wide range of devices such as smartphones, personal computers, PDAs, laptops, tablets and other handheld embedded devices. As communication and internet technology continue to advance rapidly, our daily lives are increasingly immersed in this virtual world. Security is the most important concern in IoT networks. Physical security prohibits unauthorized access to servers, storage and network devices Network security prevalent illegal access to network data as well as tampering with or unlawful alteration concerned with security at software level. Within IoT networks, the Application layer plays a critical role. It is responsible for delivering specific services and functionalities to end users. The application layer interfaces directly with users and is where the actual data processing and service execution occur. The application layer, being the point of interaction between users and devices, is particularly vulnerable to various threats. These include data breaches, unauthorized access, and malicious attacks, which can lead to significant privacy violations and security breaches. The layout of this paper follows. In section [2] IoT Framework and Security Challanges are addressed with different layer threats. In contrast, Section [3] Application Layer Security Analysis with some case studies while Section [4] is used for conclusion.

[2] IoT FRAMEWOK AND SECURITY ANALYSIS

The internet of things (IoT) architecture typically consists of five key layers : Perception, Transport, Processing, Application, Business Layers. Each layer has distinct role, the transport layer is crucial for data communication, where data is exchanged across networks. However, this exchange in the public domain makes the data susceptible to unauthorized excess or theft. For example, there is IoT based system in smart farming, where after sensing moisture, a sensor sends data to cloud. On the behalf of that data, irrigation is planned for plants accordingly. If data is theft or changed then there is a strong possibility of a loss of data and it will affect the economy of farmers, because of irregularity in irrigation. To address this issue, it’s essential to implement robust security measure that protect the data during its journey from the sensor to the cloud and then from the cloud to the end-user. This ensures that the transmitted data remains confidential, integral, and secure, thereby safeguarding the operational integrity and economic stability if IoT systems in application like smart farming.

These are some security issues at different layers of IoT networks (Fig.1).



Business Layer — Manages the whole IoT system, including applications, profit models, etc — Authentication Flag and Privilege escalation, Business Flow Bypass etc

Application Layer — Responsible for delivering application services to the users via user interfaces. — Client App, Data Leakage, Malicious code Integration, Data Alteration etc.

Processing Layer — Stores, analyzes, and processes data coming from the transport layer. — Authentication, Authorization, Data Manipulation etc.

Transport Layer — Transfers the data from perception layer to processing layer. — Eavesdropping, Data Transit Attacks, Back Door Attack, Pharming etc.

Perception Layer — Is the physical layer which contains sensors to gather data. — Tempering, Denial of Service, Physical Attack etc.

Fig: IoT Framework Layers With Security Concerns

Fig. 1: IoT Framework Layers with Security Concern

[3] APPLICATION LAYER SECURITY ANALYSIS

In IoT layered architecture, if the perception layer is compromised, it exposes vulnerabilities in higher layers like the transport layer, which in turn affects the application layer. However, an attack on the application layer doesn't directly impact lower layers. Despite this, the application layer, designed for human interaction, faces more threats due to its exposure to both benign and malicious actors. This disclosure is a key difference between the application layer and the other layers of the IoT layered Architecture. One of the fundamental information security principles that must adhere to when protecting any application at the application layer is CIA-Triad. While this might sound like something you would find in the arsenal of a secret government agent, in computer science it’s just an acronym that stands for confidentiality, integrity, and availability. There should be a sure that the data is secret, that has not been tampered with in any way, and that it is available to the people who should access it.

The system architecture incorporates the security of the IoT application layer, which includes IoT apps and application layer protocols. The cornerstone for communication between diverse IoT use cases, devices, and operating services is IoT application layer protocols. To put it another way, IoT application layer protocols serve as a bridge between IoT use cases and end consumers. Security at this layer is therefore essential given the significance of the application layer in all IoT use scenarios. In addition, it’s likely that hackers in the IoT application layer would violate privacy through a variety of methods, including cross-site scripting, injection, and unauthorized access assaults. The application layer interacts with and serves end users directly. This layer contains IoT applications such as smart homes, smart meters, smart cities, smart grids, and many more. This layer has unique security vulnerabilities not seen in other layers, such as data theft and privacy concerns. The security vulnerabilities in this layer are likewise application specific.

Many IoT applications additionally have a sublayer between the network and application layers, which is commonly referred to as an application support layer or middleware layer. The support layer provides numerous business services and aids in resource allocation and computation. Most security issues encountered at the application layer are discussed below.

1. DoS Attack: A Denial-of-Service (DoS) attack is an attempt to bring a machine or network to a halt, rendering it unreachable to its intended users. DoS attacks achieve this by flooding the target with traffic or providing it with information that causes it to crash.

Smart Healthcare: Wearable devices in smart health systems track vital signs like blood pressure, temperature, heart rate, and blood sugar, storing data as Personal Health Records (PHR) on cloud servers for physician analysis. Given the sensitive nature of this data, privacy is a critical concern in healthcare IoT applications. A major threat is a Denial of Service (DoS) attack, where attackers overwhelm the system with false traffic, disrupting normal operations and making it inaccessible to legitimate users. Such attacks can alter patient data, send misleading health information, or create fake records, potentially leading to misdiagnoses, inappropriate treatments, or false emergency alerts. In severe cases, these actions could result in life-threatening situations for patients.

Smart-City: As the name suggests, the main purpose of DoS attacks is to prevent potential users of smart city applications from accessing system resources or services. DoS attacks can target the network layer or the application layer. DoS attacks could adversely affect smart city applications that provide centralized surveillance services.

2. Eavesdropping Attack: A sniffing or snooping attack, often known as an eavesdropping attack, is the stealing of information while it is transmitted across a network by a computer, smartphone, or another connected device. The attack uses unsecured network communications to gain access to data as it is sent or received by its user.

Smart City: Eavesdropping is an example of a passive attack in which an attacker attempts to eavesdrop on unsecured communications between two or more parties in order to gain access to data. In front of smart cities, eavesdropping is a serious threat as it can compromise system integrity and confidentiality.

Smart Grids: Smart grids are vulnerable to various security threats targeting their confidentiality, integrity, availability, and privacy. Attacks like eavesdropping, illegal access, and password theft seek to steal sensitive information. Meanwhile, data tampering, spoofing, and man-in-the-middle (MitM) attacks focus on corrupting or altering data. Disruptive actions such as jamming, Denial of Service (DoS), and buffer overflow attacks aim to make grid services unavailable.

Additionally, technologies like Advanced Metering Infrastructure (AMI) can lead to privacy violations by exposing sensitive user data. Robust security measures are essential to safeguard the reliable operation of smart grids.

3. Masquerade Attack: A masquerade attack is one in which a fictitious identity, such as a network identity, is used to gain unwanted access to private information via valid access identification. If an authorization procedure is not completely secure, it might become particularly vulnerable to a masquerade attack.

Smart City: Refers to situations where malicious users can gain unauthorized access to a system and steal information about fake identities (devices, entities, etc.).

Smart Agriculture: Smart farming relies on IoT sensors and smart meters to monitor data like humidity, temperature, and water quality. This data is sensitive because its analysis can reveal valuable insights, making it a target for unauthorized access and security threats, such as insider and cloud data breaches. Authentication issues also pose risks, where malicious users or programs can impersonate legitimate identities to gain system access. Additionally, smart farming systems are vulnerable to data integrity attacks, which can allow unauthorized modifications to critical information, like the pH of agricultural water.

4. Message Modification Attack: It indicates that a component of a communication has been manipulated, or that the message has been delayed or reordered in order to have an unlawful effect. Modification is an attack on the original data’s integrity. It basically means that unauthorized parties not only obtain data but also spoof it.

Smart City: In this attack, an intruder attempts to modify message headers (such as changing message destinations) or data (such as injecting malicious content) to cause unexpected behavior in system performance. Message modification attacks can also cause system delays, congestion, and compromise data integrity in smart city applications.

5. Traffic Analysis Attack: The attacker does not have to compromise the real data in this form of assault. Simply listening to network communication allows the attacker to undertake traffic analysis to establish the location of important nodes, the routing structure, and even application activity patterns.

Smart City: In a traffic analysis attack, an attacker monitors and analyses network traffic to identify existing patterns (e.g. when a particular user sleeps/wakes up), metadata (e.g. when/how packets are sent). and useful information. Traffic analysis is a passive attack that can compromise the confidentiality of smart city information.

Smart Farming: Data acquired from various sensors is the foundation of a smart farm, where most decisions are automated based on the data. For instance, the smart farm's irrigation system activates and deactivates based on the soil water level measured by the moisture sensors. This can be analyzed by the traffic analysis attack.

6. Malware: Malware, often known as malicious software, is any program or file that is designed to do damage to a computer, network, or server. Malware can take the form of computer viruses, worms, Trojan horses, ransomware, and spyware.

Smart City: This type of threat refers to attacks on software programs that can perform unauthorized actions (illegal access, information theft or modification, etc.) on infected systems. In smart cities, CCTV systems are a prime example where malware can access systems to view sensitive information and security context such as private homes and banks.

Smart Healthcare: One of the most serious new hazards in healthcare is malware that affects medical devices. If a medical device, such as a bedside monitor, becomes infected with a computer virus, it can do one of two things: it can break and so be unavailable to provide patient care, or its performance becomes less predictable.

7. Disinformation Attack: Disinformation attacks are the deliberate spread of false information with the objective of deceiving, confounding or manipulating an audience. These attacks are frequently used to modify attitudes and ideas, advance a specific agenda, or force specific actions from a target audience.

Smart City: In this type of attack, an attacker intentionally disseminates false data (such as sensor reading data) in order to influence the outcome or mislead the behavior of users of the system. In smart cities, disinformation attacks can lead to consequences ranging from delays to unnecessary congestion.

Industrial IoT (IIoT): Security threats in Industrial IoT (IIoT) encompass various attacks, including injecting adversary code to manipulate industrial machinery, jeopardizing safety. In IIoT, confidentiality safeguards data from unauthorized access, vital to protect customer and supplier information and trade secrets. Malware poses a significant risk by breaching confidentiality in IIoT systems, potentially exposing sensitive data.

[4] CONCLUSION:

This study underscores the criticality of securing the IoT application layer. While extensive research has explored IoT security comprehensively, limited attention has been paid specifically to the security aspects of the IoT application layer. A thorough classification of key security requirements, threats, and existing solutions is essential for advancing IoT use cases, protocols, and overall security. The study identifies six fundamental security needs for the IoT application layer: confidentiality, integrity, availability, authentication/authorization, non-repudiation, and privacy, including defenses against DoS attacks. Adhering to these security standards ensures proper IoT system operation and shields against potential attacks and vulnerabilities. Moreover, increasing user awareness about the security risks associated with IoT device ownership and usage is imperative.

REFERENCES:

[1] Top 5 IoT security threats and risks to prioritize", https://www.techtarget.com/iotagenda/tip/5-IoTsecurity-threats-to-prioritize, 04 Apr 2022.

[2] S. Sontowski, M. Gupta, S. S. Laya Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, and R. Sandhu, "Cyber attacks on smart farming infrastructure," in 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, pp. 135–143.

[3] Security and Privacy Issues in IoT (December 2016) International Journal of Communication Networks and Information Security 8(3):147-157

[4] IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020 263 Manuscript received April 5, 2020 Manuscript revised April 20, 2020 "A Review on Security and Privacy Issues and Challenges in Internet of Things."

[5] "Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions." MAHMOUD ABBASI 1, (Member, IEEE), MARTA PLAZA-HERNÁNDEZ1, JAVIER PRIETO 1, (Senior Member, IEEE), AND JUAN M. CORCHADO1,2,3

[6] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in vanet security: a survey," in 2015 IEEE 82nd vehicular technology conference (VTC2015-fall). IEEE, 2015, pp. 1–7.

[7] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the internet of things for smart healthcare," IEEE Communications Magazine, vol. 56, no. 4, pp. 38–44, 2018.

[8] Debabrata Singh, Pushparaj, Manish Kumar Mishra, Anil Lamba, Sharabanee Swagatika, "Security Issues In Different Layers Of IoT And Their Possible Mitigation",International Journal Of Scientific & Technology Research, Volume 9, Issue 04, APRIL 2020.

[9] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (ntma): a survey," Computer Communications, vol. 170, pp. 19–41, 2021.

[10] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," Journal of Manufacturing Systems, vol. 47, pp. 93–106, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612518300463.