CYBER SECURITY PENETRATING INVESTIGATION OF IOT SECURITY ISSUES AND CHALLENGES

Abstract

The Internet of Things is quickly affecting a number of areas of our daily life, such as household appliances, transportation, industry, education, agriculture, hospitals, environmental monitoring, etc.

Any technology's primary attributes are its security, privacy, authentication, and user-friendliness. IoT security is primarily concerned with authentication, confidentiality, and access control. Security, trust, and confidentiality are essential for assuring users' happiness. NFC, RFID, and WSN are a few of the methods for managing IoT security, privacy, and trust. However, the absence of comprehensive security solutions in a number of vertical application fields hinders the development of IoT systems. The top ten areas that need to be secured from a security and privacy standard point of view for IOT devices to fill this gap will be the topic of this research study.

KEYWORDS: Wireless -Networks, Mobile- Networks, Certificate-based Authentication, Renewable Security, Penetrating investigation, IOT, Security Issues

Authors

Dr. Govindraj Chittapur
Department of Computer Science and Engineering
Basaveshwar Engineering College, Bagalkote
gbchittapur@gmail.com

Dr. V. B. Pagi
Department of Computer Science and Engineering
Basaveshwar Engineering College, Bagalkote
veereshpagi@gmail.com

Dr. S. V. Saboji
Department of Computer Science and Engineering
Basaveshwar Engineering College, Bagalkote
sabojishivakuamar@gmail.com

I. INTRODUCTION

Within the realm of the Internet of Things (IoT), a groundbreaking paradigm emerges, enabling the internet to seamlessly interface with physical objects in the tangible world. Consequently, this interconnected landscape fosters a continuous exchange of information and services, bringing together people and devices in innovative ways. The advent of IoT quietly integrated itself into our daily lives over the past decade, primarily facilitated by the proliferation of wireless communication systems like RFID, WiFi, 4G, and IEEE 802.15.x, which have increasingly driven intelligent monitoring and control applications.

It's heartening to witness substantial investments in the IoT vision from industry leaders, including manufacturers, service providers, and software developers. Gartner predicts that, by 2030, the installed base of IoT devices will surge from 1.6 billion to 3.2 billion, driven by government and utility initiatives.

The proliferation of ubiquitous and cost-effective sensors has transformed physical data into digital content, propelling steady growth in the IoT market as billions of devices, services, and systems interconnect. IoT applications that yield savings in fuel, energy, and labor often demonstrate significant financial impacts and rapid payback periods. Projections suggest the IoT market will exhibit a robust year-over-year growth rate of 15.4%, reaching a value of US$1.1 trillion by 2025.

Anticipating the year 2030, it is forecasted that IoT devices will generate an astounding 100 zettabytes of data. To harness insights and enhance operational efficiency, sensors and gateways transmit data to centralized platforms, where it undergoes aggregation, processing, storage, analysis, and visualization. While centralized architectures offer advantages, such as scalability and efficiency, they also present limitations, including higher data exchange latency, delayed response to actionable intelligence, vulnerability to environmental disasters, susceptibility to security breaches, elevated infrastructure costs when expanding to new locations, and constrained adaptability of devices designed for specific tasks due to standardized hardware.

Considering these drawbacks, computing platforms are undergoing a transformation from centralized to distributed and decentralized architectures, with an emphasis on fog computing and artificial intelligence closer to data sources. By leveraging a combination of IoT, fog computing, big data analytics, and cloud technology, this knowledge paper showcases illustrative use cases. Furthermore, it recognizes the wealth of data accessible through web-connected systems, coupled with their capacity for self-enhancement through artificial intelligence.

The benefits of increased efficiency through the use of Internet of Things (IoT) technology across various industries include:

1. **Manufacturing Efficiency:** IoT sensors in factories can identify bottlenecks, reduce production time, and minimize waste. Predictive maintenance, based on advanced sensing and analytics, helps schedule machine servicing only when necessary, reducing costs and downtime.

2. **Asset Tracking:** IoT enables real-time tracking of assets, monitoring performance, optimizing workflows, and attaching sensors to both large and small assets. Examples include tracking boats' status remotely and efficiently locating vehicles at auction locations.

3. **Energy Efficiency:** IoT aids in significantly reducing energy consumption by analysing data from sensors like lighting, temperature, and energy usage. Companies like Google have cut energy expenditures in data centres by 15% using IoT-driven intelligent algorithms.

4. **Agricultural Efficiency**: IoT technology helps outdoor agriculture by sensing soil moisture and considering weather conditions to optimize irrigation, reducing water consumption. In indoor agriculture, it manages microclimates (humidity, temperature, light) to maximize production.

5. **Inventory Management:** IoT tags on individual products enable efficient tracking of items in large warehouses, reducing labour costs and search time. In retail, real-time inventory data helps optimize product ordering and reduce the costs of holding excess inventory, eliminating manual inventory checks.

Overall, IoT enhances efficiency by either increasing output with the same input or achieving the same results with fewer inputs, making it valuable across various sectors.

II. WORKSPACE OF IOT ECHO-SYSTEM

The Internet of Things (IoT) encompasses a wide array of applications and use cases, and all complete IoT systems consist of four fundamental components that work together synergistically. In Figure 1, we'll illustrate how the IoT ecosystem operates.

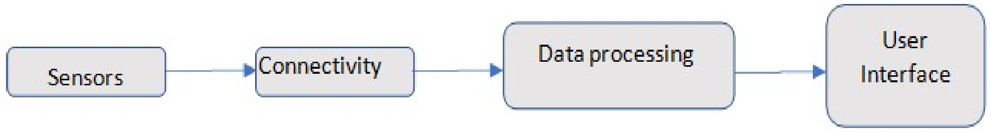

Figure 1: Workspace of IOT ecosystem

1. **Sensors/Devices:** At the heart of any IoT system are sensors or devices. These components are responsible for initially collecting data from the environment. This data can range from simple temperature readings to full-fledged video feeds. Sensors/devices can be standalone entities or integrated into multifunctional devices that go beyond mere sensing. For example, your smartphone is not just a sensor; it can perform various actions. Nevertheless, in this first stage, something is actively gathering data, whether it's a dedicated sensor or a multifunctional device.

2. **Connectivity:** The data collected by sensors/devices needs to find its way to the cloud. This connectivity is facilitated through diverse methods, such as cellular networks, satellites, WiFi, Bluetooth, low-power wide-area networks (LPWAN), gateways/routers,

or direct Ethernet connections. Each method has its trade-offs, involving factors like power consumption, range, and bandwidth. The choice of connectivity depends on the specific requirements of the IoT application, but the ultimate objective is the same: transmitting data to the cloud.

3. **Data Processing:** Once the data reaches the cloud (a topic we'll delve into in a subsequent section), software comes into play for data processing. This can entail straightforward tasks, such as verifying whether a temperature reading falls within an acceptable range. Conversely, it can involve complex operations like employing computer vision to identify objects, such as potential intruders on a property. Decisions and actions based on the data, such as responding to temperature increases or intruder alerts, come into play in the next stage, which involves the end-user.

4. **User Interface:** Data processed in the cloud becomes meaningful when presented to end-users through a user interface. Alerts, notifications, or messages (via email, text, or other means) can be sent to users. For instance, a text alert may be dispatched if the temperature in a cold storage facility rises above a certain threshold. Users can actively monitor the system through an interface, often accessible via a smartphone app or web browser, allowing them to view video feeds from various locations.

   However, the interaction is not always one-way. Depending on the IoT application, users may also have the ability to take action and influence the system. For example, a user could remotely adjust the temperature in a cold storage facility using a smartphone app. Moreover, certain actions can be automated, with the system executing predefined rules. Instead of waiting for user intervention, IoT systems can automatically notify security teams or relevant authorities in response to intruder alerts, providing a comprehensive and dynamic ecosystem of data collection, analysis, and user interaction.

III. GUIDELINES FOR IOT SECURITY

The increasing volume of data traversing networks and residing in storage systems has exposed vulnerabilities within infrastructure, rendering IoT security a paramount concern for organizations. Safeguarding data confidentiality, integrity, and availability is imperative to mitigate cyber threats and the potential for malicious exploitation.

- To bolster security, it is crucial to implement robust mechanisms and strategies for secure data communication, storage, and sharing, leveraging cutting-edge cryptographic methods and security algorithms:

- Authentication of all network entities relies on public key cryptography and X.509 certificates, authenticated by a trusted root authority. Storage of these keys and certificates necessitates the use of a hardware security module compliant with Federal Information Processing Standards (FIPS).

- Ensuring data confidentiality during transmission is accomplished through Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) encryption standards/protocols.

- Data integrity is verified through the utilization of cryptographic hashes such as the Secure Hash Algorithm (SHA).

- Messages and files bearing digital signatures instill trust in recipients, signifying the identity of the sender.

- Role-Based Access Control (RBAC) should be enforced consistently across all applications.

- IoT devices can bolster security by incorporating secure boot mechanisms.

- Classification of all data in storage systems according to security levels is imperative, with critical data, such as user authentication data, necessitating encryption.

- Rigorous security hardening of device software and firmware is essential to thwart potential backdoor entry attacks.

- Robust safeguards must be deployed to protect centralized infrastructure against Distributed Denial of Service (DDOS) attacks.

- Keeping all computing systems up-to-date with the latest security patches is essential to mitigate known vulnerabilities.

- Advanced security measures, including anti-APT (Advanced Persistent Threat) systems, Intrusion Detection Systems, Network Behaviour Analysis Tools, antivirus and antimalware systems, next-generation firewalls, security event management, email security systems, and data loss prevention systems, should be implemented in cloud and data canter environments to fortify critical IT infrastructure.

These measures collectively fortify IoT security, assuring organizations that their data and systems remain shielded from potential threats and vulnerabilities.

IV. PROBLEM STATEMENT AND ISSUES IN IOT SECURITY

IoT (Internet of Things) devices are gaining popularity across various domains, including e-home, e-health, e-commerce, e-banking, e-enterprises, e-learning, and e-trafficking. Beyond connecting computers and mobile devices, IoT extends its reach to smart buildings, homes, companies, and even entire cities. Ensuring a secure and resilient cyber security infrastructure for IoT is essential, as these devices become more prevalent in smart home environments. Additionally, IoT environments pose unique security challenges compared to traditional computer networks.

Every internet-connected sensor or device becomes a potential target for hackers, making cyber security a critical concern. Gateways can help reduce exposure by connecting only to them, but they become a primary target for attackers since they are the first line of defense.

IoT applications vary widely, from asset tracking with low data throughput to real-time surveillance with high bandwidth demands. This diversity often requires a combination of technologies to meet specific IoT solution needs.

Security measures for IoT include message encryption, transport encryption, and adherence to standards like TLS. Separate networks ensure secure and private communication between devices. Additional precautions involve firewalls, physical access restrictions to gateway devices, one-time passcodes, and disabling unnecessary OS features.

IoT systems often rely on cloud computing for data storage and processing. Cloud enables efficient data aggregation and scalability, reducing the need for extensive computational power on individual devices. The cloud serves as the central hub for IoT systems, handling data processing, commanding, and analytics.

IoT platforms play a crucial role in the ecosystem but may require clarification for some. The value of IoT lies in the data it generates, which can lead to actionable insights and improved efficiency or user experiences. Effective tools should offer descriptive analytics, visualization, diagnostics, predictive analytics, and machine learning capabilities.

Despite ongoing research into IoT security challenges, there is a need for a systematic study focused on cyber security in intelligent home-based IoT infrastructure. The expanding computing resources, attack surfaces, communication infrastructure, and attack rates associated with smart homes and IoT services bring forth significant security challenges.
This proposed chapter aims to address the security gaps in IoT cyber security, particularly in enterprise and intelligent home devices. The goal is to develop cyber security standards and guidelines to safeguard the IoT ecosystem against identified threats and attacks.

Every organization stands to benefit significantly from embracing IoT. By connecting various assets, individuals, and environments, IoT can unlock substantial organizational value and accomplish seemingly impossible feats. However, many individuals require clarification on how to implement secure IoT solutions, whether for business purposes or city planning, considering the broad and far-reaching nature of the IoT concept.

Key questions for organizations include:

- How can my business effectively implement secure IoT solutions?
- How should my city approach creating value for residents while ensuring the secure implementation of IoT technologies?

V. CHALLENGES IN IOT SECURITY

Security professionals in the field of IoT (Internet of Things) must extend their focus beyond the conventional information security principles of confidentiality, integrity, and availability. This is imperative because the expanded connectivity brought about by IoT introduces a vast and often unfamiliar attack surface. IoT devices and applications have the capability to store extensive volumes of personal, operational, and corporate data.

Among the foremost concerns for cybersecurity experts in the realm of IoT are data breaches and other cyberattacks. However, their vigilance must encompass a broader spectrum, with specific attention to securing various aspects:

1. **Connectivity Security:** Ensuring the security of IoT device connections is paramount.This involves safeguarding the communication channels to prevent unauthorized access or tampering with data in transit.

2. **Device Hardening:** IoT devices must be hardened against potential vulnerabilities and exploits. This includes regular updates, patch management, and configuration controls to reduce susceptibility to attacks.

3. **Threat Monitoring:** Continuous monitoring of IoT ecosystems is essential to detect and respond to potential threats in real-time. This proactive approach helps mitigate risks before they escalate.

4. **Security Posture Management:** Managing the overall security posture of IoT environments involves assessing and maintaining the security of all connected devices, applications, and networks to reduce vulnerabilities.

5. **Securing Cloud-Stored Data:** Given that IoT data often resides in the cloud, robust security measures must be in place to protect data stored on the backend. This includes encryption, access controls, and data backup strategies.

6. One critical consideration for IoT security professionals is the potential for IoT vulnerabilities to pose not only digital risks but also physical dangers and operational disruptions. A compromised IoT system can lead to life-threatening situations and the disruption of revenue-generating operations.

VI. CONCLUSION

In conclusion, IoT security professionals face multifaceted challenges in safeguarding IoT ecosystems. Beyond the conventional security triad, they must address connectivity, device hardening, threat monitoring, security posture management, and the protection of data in the cloud. This comprehensive approach is vital to mitigate the diverse risks associated with IoT and ensure the safety of both data and physical operations.

REFERENCES

[1] FORECAST research paper references: IOT METERS BY USE CASE, WORLDWIDE, 2020-2030, HTTPS://WWW.GARTNER.COM/EN/DOCUMENTS/3996804,

[2] India Federation of Indian Chambers of Commerce & Industry research paper references HTTPS://FICCI.IN/SPDOCUMENT/23092/FUTURE-OF-IOT.PDF

[3] CIS Controls OF IOT Companion Guide https://www.cisecurity.org/insights/white-papers/internet-of-things-security-companion-to-the-cis- critical-security-controls

[4] D. Evans and D.M. Eyers. “Efficient data tagging for managing privacy in the Internet of Things”. In: IEEE Int. Conf. on Green Computing and Communications, GreenCom, Conf. on Internet ofThings, iThings and Conf. on Cyber, Physical and Social Computing, CPSCom. Besancon, France, 2012,pp. 244–248.

[5] B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou. “Opportunistic IoT: Exploring the HarmoniousInteraction

Between Human and the Internet of Things”. In: Journal of Network and Computer Applications 36.6 , pp. 1531–1539.

[6] IOT-EST project. http://ict-iotest.eu/iotest/.

[7] Ian Welch, IoT Attacks: Features Identification and Clustering; 29 December 2020 - 01 January2021, 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

[8] Puthiyavan Udayakumar R. Anandan “Top 10 IoT Security Probing Areas”, 2023 IEEE world AI Iot Congress (AIIoT),2023