International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

xx

COPY RIGHT

IJIEMR Transactions, online available on 31th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/55

TITLE: A DECADE OF RESEARCH ON DEVICES AND CYBER ARCHITECTURES FOR IOT SECURITY

Volume 13, ISSUE 05, Pages: 519-523

Paper Authors **Tanishaq , Dr. Rishi Kumar Sharma, Gaurav Kumar, Nikita jatav**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A DECADE OF RESEARCH ON DEVICES AND CYBER ARCHITECTURES FOR IOT SECURITY

Tanishaq , Dr. Rishi Kumar Sharma, Gaurav Kumar, Nikita jatav
Student of BCA, CSE Quantum University Roorkee, India yanutyagi50@gmail.com
Associate Professor, CSE Quantum University
Roorkee, India
Student of BCA, CSE Quantum University Roorkee, India gvats760@gmail.com
Student ofBCA, CSE Quantum University Roorkee, India nitikajatav11@gmail.com

Abstract—Although it can be challenging to handle, the security of (IoT)-based smart Technology with sensors, actuators, and achievement control loops is crucial. How do they help with the development of safe IOT smart systems? Do any IoT security support architectures? Our goal is to thoroughly analyze multiple of the literature on devices and designs for IoT and privacy. We adhere to the established protocols for performing systematic reviews of literature. According to personal data, over the past three years, there has been an increase in the number of reviews about device and architecture IoT security. We are unaware of any systematic application of devices and architectures that can handle problems with network security (and privacy) or the Internet of Things (IoT)span class='highlighted color-1'¿span¿ device level in addition to the degree of architecture. Lastly, we talk about the present research gaps in this field as well as how to secure them to encourage the application of devices for privacy and security in IoT design.

Index Terms—IoT Security, Cloud Robotics, IoT Network Attacks.

I. Introduction

IoT network security must always be set up in the growing connected world of today, where smart gadgets are commonplace. This digital environment is supported by networking, allowing smooth device-to-device communication. IoT servers, essential to controlling device-to-device data exchange, are at the center of this ecosystem. The study examines how important IoT servers are to maintaining network security. These servers guarantee the integrity and privity of data handover by utilizing state-of-the-art cybersecurity measures including encryption and firewalls. Developing novel strategies to build up IoT server infrastructure will help to lower cyber threats and improve the reliability of networked systems.

II. CYBER SECURITY

Cybersecurity is like having a lock on your digital stuff. It's all about protecting your computers, networks, and data from unauthorized access, attacks, or damage. It's like putting up fences and security cameras around your online world to keep out the bad guys and your information safe and secure.

III. USE OF CYBER SECURITY

In the finance industry: cyber security is essential for protecting transactions, customers' data, and delicate data from cyber threats such as data breaches, identity theft, and fraud, including encryption, and multi-factor authentication.

governments and defense organizations face constant cyber threats from nation-state actors, cybercriminals, and activities seeking to disrupt critical infrastructure, steal classified information, or launch cyber espionage campaigns.

Critical infrastructure sectors such as energy, transportation, water, and telecommunications rely on interconnected networks and industrial control systems (ICS) to operate essential services.

Education: Educational institutions handle sensitive student and faculty data, including personal information, academic records, and research data. Cyber security measures are vital to prevent unwanted access to this data, data breaches, and cyber-attacks. security policies, access controls, and cyber security awareness training help reduce the possibility of security incidents in educational environments.

IV. Threats on IOT devices

There are many types of threats in IOT but the main one is human threat. Human threat means we do anything to curb human threats to Internet of Things devices, which are malicious attacks.

V. IoT Device Attacks

1. Node Tampering: Through physically modifying the compromised node, the attacker can extract sensitive data,including the encryption key, in this attack.

2. RFID RF Interference: The attacker uses noise signals to launch a denial-of-service attack over radio frequency signals. These signals are used for RFID communication.

3. Node Jamming in WSNs: By using a jammer, the attacker can disturb the wireless communication. It causes a Denial Of Service attack.

4. Social Engineering: The attacker physically interacts with and manipulates users of an IoT system. 4 To accomplish his objectives, the attacker gets access to private information.

5. Attack of Sleep Deprivation: The attacker aims to exert greater force which results in the shutting down of nodes.

6. Malicious Code Injection: The adversary physically introduces a malicious code into the node of the IoT system. The attacker can get full control of the IoT system.

VI. Network Attacks

1. Attacks Using Traffic Analysis: To get network information, the attacker reads and intercepts messages.

2. RFID Spoofing:An adversary spoofs RFID signals. Then it captures the information that is transmitted from an RFID tag. Spoofing attacks give wrong information that seems to be correct and that the system accepts.

3. RFID Cloning: In this attack, adversaries copy data from a pre-existing RFID tag to another RFID tag. It does not copy the original ID of the RFID tag. The attacker can insert wrong data or control the data passing via the cloned node.

4. RFID Unauthorized Access: If the correct authentication is not provided in the RFID systems, then the adversary can observe, alter, or remove information on nodes.

5. Attack of the Sinkhole: In an attack using a sinkhole, a malicious party breaches a network node and uses it to carry out the attack. By pretending to have the shortest way to the headquarters, the hijacked node informs nearby nodes via bogus routing information, drawing in traffic. Then, in addition to dropping packets, it can alter the information. The easy method of sinkhole node identification. The suggested method involves a node creating an entry in its database with the ID and hop lengths whenever it sends a packet to an adjacent node. The average hop count is then calculated, leaving out the minimum hop count, and the average and minimum values are compared.

6. Man in the Middle Attacks: The communication between the two nodes is intercepted by the attacker over the internet. They use eavesdropping to get confidential information.

7. Denial of service: An attacker overloads the network with traffic, preventing legitimate users from using services

8. Routing Information Attacks: The perpetrator of this attack can make the network complex by spoofing, modifying, or sending routing information. It results in allowing or dropping packets, forwarding wrong data, or partitioning the network.

9. Sybil Attack: In this assault, a malevolent node takes the identities of multiple nodes and acts as them. E.g. in the Wireless Sensor Network, voting system single nodes can vote many times

VII. Software Attacks

1. Phishing Attacks: The hacker uses phony websites and email spoofing to gather personal data, including usernames and passwords.

2. Trojan horses, viruses, worms, spyware, and awareness of Malicious code is one way an adversary can compromise the system. These codes are disseminated via file downloads from the Internet and email attachments. Without human intervention, the worm is capable of self-replication. To find the infection, we can utilize firewalls, methods for detecting intrusions, worm detectors, and antivirus software. It contains a honeypot to keep worms 1 removed from the system along with anomaly and signature detection. This hybrid approach employs anomaly/signature detection, honeypots, and worm protection.

3. Malicious Scripts: By injecting a malicious script, the attacker can obtain entry into the system.

Denial of Service: The attacker blocks the users from the application layer by denying services.

VIII. Encryption Attacks

1. Side-channel Attacks: The attacker uses the side-channel information that is emitted by encrypting devices. It is neither the plaintext nor the cipher text, it contains information about power, the time required to operate, faults frequency, etc. The attacker uses this information to detect the encryption key. There are several kinds of side-channel assaults such as timing attacks, Simple Analysis of Differential Power, and Differential Attacks Using Fault Analysis.

IX. Security Challenges on IOT Devices

Low-power embedded device: IoT devices have limited computation and storage capacity. It is frequently incorporated in larger hardware or wearable devices, making it difficult to perform security algorithms that are typically hefty and expensive for a resource-constrained device.

Trust Management: Trust management is critical in both inter-entity and inter-user communication. To determine a trustworthy entity, reputation must be calculated. The collective perception of a central entity aids in calculating the reputation of the other entities. The inconsistencies in reputation value can be rectified by sharing trust information from several central institutions.

Heterogeneity: IoT is the combination of multiple heterogeneous networks, hence it has its own compatibility and security challenges. It is challenging to identify trustworthy nodes in a diverse ecosystem. Heterogeneity, identity management, privacy, and fault tolerance Security IoT protocols.

Secured Access control: Within an Internet of Things network, secured access management poses a major difficulty. Cloud-based data is typically accessed by numerous entities and processes. Furthermore, different retrievers offer various degrees of granularity for getting the same data. Because of this, creating and securing Policies for access control are among the hardest jobs.

Trust Management: During the phases of data collection, dissipation, and authentication—when powerful cryptographic

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

techniques or digital signatures are recommended – trust management is essential.

Identity Management: It is necessary to uniquely identify an IoT device and give authentication and authorization for each device. Authentication ensures the legitimacy of data passing through the device, while authorization ensures safe access control. The entities in an IoT network may be added dynamically and consequently, identity management with authentication becomes even more complicated.

Privacy: It is critical to provide privacy for the billions of users in IoT networks. The anonymity of the user must be maintained. Any service provider must keep an access control list. Privacy must be given full consideration throughout the IoT life cycle.

We must utilize security on IOT devices.

X. Get Familiar with the Network in addition to using the Connected Device

A network becomes susceptible to various dangerous threats when an IoT device can access the Internet. Therefore, attackers can exploit this vulnerability and gain entry into the system. It becomes more insecure and your information is far more likely to be leaked or at least available over the internet if a greater number of devices are linked than are equipped. Our network, the device connected to it, and its vulnerability to revealing the data flowing over it must all be understood to lessen this threat. Your location and personal information are used against you by cybercriminals.

XI. Providing IoT Device Access on Your Network

Once the device has an internet connection, identify the device and The nature of the network it is utilizing or operating on. Before utilizing an IoT device, you should Observe various security patches or features (which may be concealed). Before installing or purchasing it, examine the device's security and priority. Always choose newer versions with fewer hazards and several safety features. Check the settings of the apparatus before use. You might want to change the privacy settings from default.

XII. Set Up Your Device's Settings

It is important to always adjust the device's default settings Before utilizing it, as many times devices come with unsafe safety and network configurations out of the box. Permission, weak credentials, and plenty of other settings need to be adjusted to meet your needs. Configuration always contributes to increased strength, integrity, and accessibility additionally higher functioning levels than before

XIII. Put Strong Encryption to Use

When using WiFi, confirm to choose a safe, encrypted network. Don't use public Wi-Fi since attackers might quickly find your details. Ensure that the network on which You're employed. is up to date and that it is not WPA2 but rather WEP or WPA. WPA2 is subject to reinstallation assaults, so Put in and upgrade fixes to reduce the risk to the user. Additionally, be sure to install some system settings, such as two-way authentication, to minimize the danger level while also adding an extra add-on layer of security for your gadget.

XIV. Put Physical Security Into Practice

Do not misplace your phone, especially if you have loaded all the apps necessary to operate your Internet of Things devices. Ensure that you possess a password, PIN, or similar secure method of opening it, in addition to the capacity to remotely wipe its data. One method is to set up automatic or selective backups of any device's data.

Cybercrime: In simple words, if we are using communication devices in a harmful or unlawful way to steal money, data, or other valuables is known as cybercrime.

There are many types of cybercrime: "Drug trafficking", "Online harassment", "Child pornography", "Credit card fraud", "Identity fraud" Etc.

Drug trafficking: Online drug trafficking involves the illicit sale, distribution, or trafficking of prohibited substances through digital platforms or the Internet. This nefarious practice utilizes websites, online marketplaces, social media platforms, encrypted messaging services, or other digital channels to facilitate transactions involving controlled substances, prescription medications, or other illegal drugs. Online Harassment: Online harassment encompasses the application of communication and information technologies by an individual or collective to persistently inflict harm upon another person.

XV. TYPES OF CYBER ATTACKS

Web hijacking: Web hijacking is a way to take control of anyone's website without his permission. In this case, the website owner can't do anything.

Phishing: A phishing attack is a type of cyber-attack where the attacker sends deceptive emails or forms to targeted individuals, often mimicking trustworthy entities like a fake Facebook login page or email login page. If the target clicks on these links and fills in their information, The perpetrator has access to their passwords and potentially steal sensitive data.

Email Bombing: In an email bombing attack, the attacker inundated the victim's system with a vast quantity of emails. The primary goal is to overwhelm the system's resources, leading to a potential crash or disruption of normal operation. Broken access control In cyber security threats, A crucial issue is broken access control. security vulnerability and it happens if a normal user is not authorized to access the root user's data, but a regular user can access the root user's data

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

due to a failed access control system.

Injunction : In the injunction, many kinds of cyber-attacks are available like SQL injection, and Cross-site Scripting (XSS). HTML injunction, and clickjacking attacks. note: all cyber-attacks can be cybercrimes however not all cybercrimes come under cyber attacks

XVI. Challenges of cloud robotics

Latency: A significant hurdle in cloud robotics lies in latency, which speaks of the time lapse between a robot sending a request toward the cloud and receiving a response. This delay poses considerable challenges, especially for applications that depend on immediate feedback and real-time responses.

Connectivity: Cloud robotics relies heavily on a stable and swift internet connection. Any interruptions in this connectivity can directly affect the efficiency of robots, resulting in delays and errors in their performance.

Security: Cloud robotics presents numerous security concerns. Internet-connected robots are susceptible to cyber threats, exposing them to potential attacks. Malicious entities may exploit these vulnerabilities to either pilfer sensitive data or gain unauthorized control over the robots.

Privacy: In cloud robotics, extensive data gathering and execution are integral. This data encompasses various sensitive categories, including personal and confidential business information. Maintaining the confidentiality and security of such data is paramount. Cloud Infrastructure: Cloud infrastructure encounters periods of downtime or encounters issues, which can disrupt robot operations, resulting in delays and potential financial setbacks.Implementing backup plans is essential to mitigate the dangers connected to relying solely on cloud infrastructure.

XVII. Architecture of Security for IOT Devices

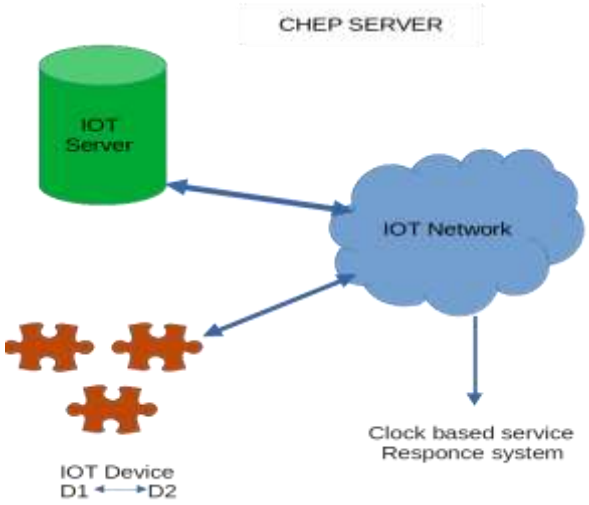

Fig. 1. Security Architecture of IoT Devices

ing device authentication and authorization, and leveraging emerging technologies such as blockchain and edge comput- ing. Additionally, collaboration between industry stakeholders, government agencies, and cybersecurity experts is essential to establish comprehensive security frameworks and standards for IoT.

XIX. CONCLUSION

The Internet of Things (IoT) explosive growth span class='highlighted color-13'¿span¿ devices has revolutionized connectivity and convenience across various sectors, from healthcare and manufacturing to transportation and smart homes. However, alongside these technical advancements comes the critical issue of cybersecurity. 9 It is critical to defend IoT devices from cyberattacks to secure sensitive data. Preserving user privacy, and ensuring the reliability of systems that are connected. In conclusion, IoT device cybersecurity is not merely a technical challenge but a multifaceted endeavor that requires collaboration among stakeholders, including manufacturers, developers, regulators, and end users. By putting security safeguards in place for the device at every turn, fostering awareness among consumers, and establishing robust regulatory frameworks, we can mitigate the dangers connected to IoT devices and realize the full potential of this transformative technology. Embracing a proactive and comprehensive method of IoT cybersecurity is necessary for building trust, resilience, and sustainability in our increasingly interconnected world.

If we assume that in a chap server, A is the IOT server (sender) and B is the IOT devices (receiver) who exchange data sent between them, but it's been found many times that data sent directly by the server to the device Then it gets stolen by hackers so we should use such a network between server and device it is predicated on CLOCK BASED SERVICE RESPONSE SYSTEM

XVIII. Cybersecurity Solutions for IoT

To enhance the security of IoT deployments, a multi-faceted approach is required. This includes implementing secure-by- design principles, conducting regular security audits, enforc-

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

REFERENCES

[1] Godwin Olaoye Fred Williams, "Cybersecurity and AI-based threat detection in the financial system", (2024) Abdullah T. Alanazi, "Clinicians' Perspective on healthcare Cybersecurity and Cyber Threats ", (2023)
[2] "Prospects and Potential Impacts of Cloud Robotics In Improving Agricultural Farm Produce: A Case of India" ,IJIEMR,International ELSEVIER SSRN, 2024.
[3] "Cloud Robotics Cybersecurity: A Novel Survey on Cloud-Based Robotic Platform for Network Security",Robotics eJournal SSRN ELSEVIER,2023.
[4] Samuel Addinigton, "ChatGPT and Cybersecurity Threats ", (2023) Joao Pedro Cunha, "Cybersecurity Threat for a Web Development"
[5] "Identity Based Remote Device Authentication system for Enhancing the Security among Remote Machines in IoT or Cloud Robotics Network", Neuro Quantology,2022.
[6] Md jobair Hossain Faruk, Sharaban Tahora, Masrura Tasnim, Hossain Shahriar, Nazmus Sakib, "A Review of Cybersecurity: Threat, Risk and Opportunities ", Ghulam shabir, Akhtar Abbas, "Cybersecurity Threat in the Internet of Things (IoT) Era: Challenges and Countermeasures ", (2024)
[7] "https://www.analyticsinsight.net/cloud-robotics-capabilities-and-challenges"
[8] "https://www.britannica.com/topic/child-pornography"
[9] "https://www.drishtiias.com/daily-updates/daily-news-analysis/role-of-the-internet-in drug trafficking"