IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 1 (Mar. – Apr. 2024), PP 21-24
www.iosrjournals.org

Impact Of Internet Of Things (IOT) Devices On Network Security At Financial Institutions

Yamini Kannan
New York, United States

Abstract –
This paper provides an in-depth examination of the network security threats associated with Internet of Things (IoT) in the financial industry. Due to the rapid adoption of IoT devices for optimizing operations and enhancing services, financial institutions have seen an enlarged attack surface for potential cyber threats. The paper explores specific serious dangers, such as Distributed Denial of Service (DDoS) attacks, data breaches, and vulnerability exploits, with a particular emphasis on the risks and implications of DDoS attacks. It offers an analysis of significant case studies and how they reflect the severity of these threats. Comprehensive mitigation strategies to secure IoT devices from such risks are also proposed, including but not limited to robust encryption practices, regular audits, and network traffic monitoring. The paper argues that while IoT brings numerous advantages to financial institutions, adequate and ongoing attention to network security must be mandated to balance innovation with robust defense strategies, thus ensuring the secure functioning of these institutions in a digital and interconnected era.

Keywords—*Network Security, Internet of Things (IoT), DDoS attacks, Cybersecurity, Financial institutions, Risk Mitigation*

Date of Submission: 24-02-2024 Date of Acceptance: 04-03-2024

I. INTRODUCTION

The Internet of Things (IoT) represents a network of interconnected devices that exchange data over the internet. These devices, embedded with sensors, software, and other technologies, expand beyond traditional computing devices like smartphones and laptops to include an assortment of devices such as Automated Teller Machines (ATMs), smart surveillance cameras, door access controllers, motion detectors and sensors, smart locks, tablets, temperature sensors used in data centers, asset tracking devices, biometric authentication devices, wearable devices for mobile payments, smart card readers, and mobile point of-sale devices

These IoT devices can provide banks and other financial institutions with real-time data, thereby enhancing decision- making capabilities, improving customer experience and operational efficiency. Financial institutions have integrated IoT extensively into their daily operations, with door access controllers managing physical access to key areas, surveillance cameras detecting suspicious activities, and tablets streamlining the customer experience. ATMs, one of the earliest IoT devices in the banking sector, provide customers with 24/7 access to their banking needs, and wearable devices now enable even more seamless mobile payments.

However, as IoT continues to expand within the financial services ecosystem, it significantly increases the potential attack surfaces for hackers. This widespread interconnectivity opens up new avenues for cyber-attacks, necessitating robust network security measures to safeguard sensitive financial data. Balancing innovation with security stands as a unique challenge and opportunity for financial institutions in the age of IoT..

II. IOT-RELATED THREATS TO NETWORK SECURITY

The integration of IoT devices into financial institutions invariably introduces various potential threats to network security. The extensive incorporation of interconnective technology has increased the attack surface for potential hackers, leading to a surge in sophisticated cyber threats. This section discusses some of these significant threats:

- Device Vulnerabilities: IoT devices often lack robust built-in security features due to their design for minimal computational load. This makes them potential weak links in a network, susceptible to cyber-attacks that could compromise the whole system.
- Lack of Encryption: Many IoT devices do not have data encryption capabilities. Thus, the data they transmit across networks is left unencrypted and vulnerable to interception. A hacker gaining access to this unencrypted data could exploit it for personal gain, cause data breaches, or disrupt operations.
- Data Privacy Concerns: As IoT devices collect and share vast quantities of data, often including potentially

sensitive information, they pose significant data privacy risks, particularly if this data falls into the wrong hands.

- Insecure Interfaces: IoT devices frequently have web-based management interfaces with poor security measures, making them susceptible to hacking and unauthorized access.
- Software Updates: IoT devices typically lack regular software updates and patches, making them an attractive target to cybercriminals who can exploit known vulnerabilities.

III. CASE STUDY 1: A STUDY ON IOT DEVICE THREATS AND COUNTERMEASURES

An investigation headed by industrial and IoT cybersecurity firm Claroty unveiled alarming security vulnerabilities in Akuvox's smart intercom product, E11. Over a dozen serious susceptibilities were discovered, including weak encryption, hardcoded cryptographic keys, insecure password recovery mechanisms, and hidden vulnerability points. These could be exploited challenging privacy laws, especially in sensitive environments like healthcare institutions. The flaws identified were labelled as 'critical' and 'high' severity, indicating a potential threat to data security and privacy since they could grant attackers remote control over the device. Silent over the year since the discovery, Akuvox announced that vulnerabilities are now their top priority, positing a firmware update release for March 20, 2023, as the proposed resolution. In the interim, the firm advised the adoption of recommended mitigations like limiting devices' internet exposure and isolating them from an enterprise network, demonstrating the need for constant vigilance and responsiveness in the rapidly evolving landscape of IoT security.

IV. CYBER ATTACKS ON FINANCIAL INSTITUTIONS

Financial institutions find themselves at the epicenter of the cyber risk landscape for several compelling reasons. At the most fundamental level, they are attractive to cybercriminals because of their direct link to financial gain. Operationalized correctly, cyber-attacks on these institutions represent lucrative ventures for hackers intent on monetary theft. Further understanding lends to the fact that these institutions are treasure troves of sensitive customer data, which includes personal, financial, and transactional information. The theft of such data opens avenues for further criminal activity, such as identity theft or fraud.

Additionally, banks and financial institutions are fundamental to the functioning of national and global economies. Disrupting their operations, therefore, can cause significant economic, political, or societal instability. In some cases, threat actors are politically motivated, seeking to destabilize economies or instigate widespread chaos and uncertainty. In the age of digitization, financial institutions are embracing new technologies to improve operational efficiency and customer experience. With the adoption of digital banking, mobile apps, and IoT devices, the cyber- attack surface has broadened immensely. This digital surface provides hackers with new, constantly evolving vulnerabilities to exploit.

Despite having some of the most robust security measures in place, the complexity and interconnectivity of the IT infrastructures within financial institutions complicate their defense structures. The challenge lies in securing every component, as attackers often target the weakest link in these complex structures, which could be an overlooked server or a human error. Lastly, some financial institutions continue operating on outdated legacy systems. These systems, built for a different era, often lack the advanced security mechanisms necessary to protect against modern cyber threats, thereby presenting yet another vulnerability that nefarious actors can exploit.

Therefore, assuming a proactive stance is essential for these institutions. This includes adopting comprehensive security measures, staying updated on potential threats, performing regular risk assessments, and constantly educating employees and customers about emerging threats and security best practices.

V. AN OVERVIEW ON RECENT IOT RELATED ATTACKS

In recent years, with the significant rise of IoT, cyber-attacks on financial institutions have taken on an increasingly sophisticated and varied form. Here's an overview of some common types of attacks that exploit IoT vulnerabilities.

- A DDoS Attacks: Distributed Denial of Service (DDoS) attacks have continued to plague financial institutions. Attackers often use botnets of compromised IoT devices to overwhelm banking servers with traffic, causing them to crash and disrupt the services [1]. These attacks are often conducted as a distraction while another fraudulent activity, like a data breach or unauthorized fund transfer, is undertaken.
- Point of Sale (POS) Breaches: With IoT-enabled POS systems now commonplace, there have been cases where cybercriminals have infiltrated these networks, installed malicious software, or intercepted transaction data to steal valuable credit or debit card information. This data is often sold on dark web markets for financial gain.
- Surveillance System Hacks: The breach of security and surveillance systems is another prime example. Modern

security systems, often connected to a larger network for ease of monitoring, can be breached to circumvent security, gain physical access, or to use the streaming hardware to launch further attacks within the network.

- ATM Skimming and Jackpotting: Cybercriminals are exploiting network-connected IoT devices, such as ATMs. They employ tactics like skimming (stealing card data during a legitimate ATM transaction) and 'jackpotting' (manipulating the machine to dispense all its cash). This holds especially true for older ATMs running on outdated software.
- Smartcard Reader Attacks: Attacks on IoT-enabled smartcard readers, used for making payments or accessing secure areas, also pose a serious concern. Moreover, as these devices are often connected to the central network, a single breach can give cybercriminals access to the larger network.
- Biometric System Hacks: More financial institutions are adopting IoT-enabled biometric systems for secure authentication. However, hacks targeting these systems represent a significant threat because it's challenging, if not impossible, to change biometric data (fingerprints, iris patterns) if they're compromised.

VI. CHALLENGES IN IMPLEMENTING IOT SECURITY MEASURES

Implementing robust security measures for IoT devices in financial institutions poses significant challenges. Notably, the diversity and complexity of IoT devices, varying from different manufacturers and systems, make it difficult to integrate them seamlessly into a single coherent security network. This means that each potentially vulnerable device could require its unique mitigation strategy, further complicating the issue. Adding to this complexity is the lack of streamlined regulation and standardization of IoT devices. As the industry rapidly evolves, it often leaves a confusing landscape of security recommendations and best practices that can be difficult to navigate. The focus on functionality over security in the development of many IoT devices leaves them lacking in comprehensive built-in security features, ultimately making them more susceptible to cyber threats. Moreover, monitoring network traffic in an IoT network can prove to be a daunting task. Tracking the immense amount of data transmitted by numerous devices is crucial for detecting and responding to potential security breaches promptly. The logistical challenge of ensuring that all IoT devices receive timely software updates is another obstacle to maintaining a robust IoT security framework, especially given that some devices may not have the capability for remote updates[5]. Finally, the expense of introducing and managing comprehensive security measures for IoT devices is considerable. Potential costs include not just the financial outlay to purchase and install security software and hardware but also the ongoing costs of training, monitoring systems, and regularly updating security measures. Despite these substantial challenges, they are not insurmountable. Advancements in technology, coupled with a proactive approach to understanding and mitigating potential risks, can provide a pathway to using IoT's benefits while minimizing exposure to cyber threats.

VII. MITIGATION OF CYBER ATTACKS : DDOS ATTACKS

IoT security measures must be comprehensive and cover a wide range of possible attack vectors. This includes employing encryption for data in transit and at rest, performing regular security audits and vulnerability testing, ensuring strong authentication and authorization controls, and creating contingencies for incident response and recovery. However, while these overall measures contribute to enhancing the security posture of IoT devices within financial institutions, focusing on specific attack types can yield in- depth insights that are increasingly critical in reinforcing cybersecurity measures in place.

In this study, we will be focusing on Distributed Denial of Service (DDoS) attacks. DDoS attacks represent a significant threat to financial institutions. In a DDoS attack, a network, service, or server is overwhelmed by a flood of internet traffic, leading to slowed down services or a complete outage. IoT devices, often co-opted into botnets, are commonly exploited to launch such attacks [1]. Given the widespread utilization of IoT devices in the financial sector, the industry is particularly vulnerable to these types of attacks.

Several strategies can be employed to mitigate the risk and potential impact of DDoS attacks on IoT devices:

- At the device level, one of the most fundamental steps is to secure each IoT device better. Devices should be configured to minimize potential entry points for attacks, which signifies disabling unnecessary services and ensuring that the default passwords on all devices are changed to strong, unique passwords. Regular updates and patches provided by manufacturers should be applied to IoT devices promptly to address any known vulnerabilities.
- On a network level, the implementation of intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help identify and block potential DDoS attacks. Traffic monitoring can also play an integral role in detecting any unusual spikes in activity, which may be indicative of a DDoS attack. As soon as an attack is detected, the traffic can be redirected to a 'scrubbing center', where the attack traffic is cleaned before re-entering the network.

- Apart from reactionary measures, proactive strategies such as improving network architecture can also help in mitigating DDoS attacks. Adopting a distributed network architecture can ensure that traffic loads are balanced and that no single point of failure exists. These also provide a level of redundancy if one server goes offline under attack, others continue to operate, negating the effects of the DDoS attack.
- Another preventive measure is regular stress testing of networks to identify potential points of weakness within the system before they can be exploited in a real-world DDoS attack [2].
- Making use of cloud-based DDoS protection services can serve as a viable mitigation technique, leveraging the cloud's substantial bandwidth resources and its inherent distributed nature that allows for effective traffic filtering and attack absorption.
- Lastly, cooperation with Internet Service Providers (ISPs) to implement traffic filtering can help block malicious traffic before it reaches the target network.

While these strategies cannot provide absolute protection against DDoS attacks, they can significantly reduce the risk and potential impact on financial institutions' IoT devices. Mitigating DDoS attacks, complex and continual though they may be, is an attainable goal. A proactive approach to security that includes implementing robust measures, continuous monitoring, and timely response to threats can create a defensive framework that minimizes damage and deters future attacks

VIII. FUTURE OF IOT AND NETWORK SECURITY IN FINANCIAL INSTITUTIONS

The future of IoT in financial institutions promises a path of innovation and improved efficiencies, but with it comes the imperative need for robust network security. As financial institutions continue to adopt IoT devices to deliver enhanced services and gain operational insights, effectively managing the corresponding security risks is crucial. Harnessing the advantages of IoT requires steps like the integration of disparate systems, facilitating smoother data flow, and unlocking potential benefits such as real-time service improvements and targeted client offerings. Meanwhile, financial institutions need a multifaceted approach to secure their networks and guard against potential cyber threats, while maintaining compliance with regulatory standards.

Machine Learning (ML) and Artificial Intelligence (AI) technologies can play a leading role in achieving this balance [2]. The use of AI and ML for real-time threat detection and prevention allows financial institutions to adapt quickly to new threats and anomalies. These technologies can recognize unusual patterns in network traffic [3], detect potential vulnerabilities in the IoT image stack, and apply advanced analytics to predict and prevent breaches before they occur [4].

Simultaneously, enhancing endpoint security by securing each IoT device and facilitating regular firmware updates can amplify defense systems. Employing encryption for data transfer, adopting a zero-trust security framework, and ensuring rigorous authentication protocols can further guard against potential breaches. Ultimately, the future of IoT and network security in financial institutions revolves around leveraging technological advancements, augmenting network and endpoint security, maintaining compliance with continually evolving regulatory standards, and cultivating a culture of security awareness throughout the organization. A deliberate, adaptive, and proactive approach to security will enable financial institutions to harness IoT's potential while effectively mitigating the associated risks.

IX. CONCLUSION

In conclusion, it's clear that the pervasive integration of IoT devices within the financial sector, although groundbreaking, also brings about significant network security challenges. The eclectic assortment of IoT devices widens the attack surface, making institutions more vulnerable to cyberattacks such as DDoS attacks. However, these threats are not insurmountable. With the right security measures, such as employing strong encryption techniques, enhancing authentication, and regular network monitoring, it is possible to mitigate potential threats. In particular, proactively addressing DDoS attacks, which pose a formidable threat to the financial sector, can bolster the overall security posture. A layered defensive framework, including device and network- level protections, load balancing, regular stress testing, and utilizing cloud-based solutions, can help guard against DDoS attacks. Continuous commitment to understanding and mitigating potential risks can, therefore, ensure a secure digital banking environment, marking the way forward in this IoT-driven era..

REFERENCES

[1] Resul, D. A. S., & Gündüz, M. Z. (2020). Analysis Of Cyber-Attacks In Iot-Based Critical Infrastructures. International Journal Of Information Security Science, 8(4), 122-133.J. Clerk Maxwell, A Treatise On Electricity And Magnetism, 3rd Ed., Vol. 2. Oxford: Clarendon, 1892, Pp.68–73.

[2] Alsamiri, J., & Alsubhi, K. (2019). Internet Of Things Cyber Attacks Detection Using Machine Learning. International Journal Of Advanced Computer Science And Applications, 10(12).Alsamiri, J., & Alsubhi, K. (2019). Internet Of Things Cyber Attacks Detection Using Machine Learning. International Journal Of Advanced Computer Science And Applications, 10(12).