Sri Lanka Institute of Information Technology (SLIIT)

ICS Assignment

Mitigating Man-in-the-Middle Attacks in IOT Systems

IT23586116 – LUTHFI H P

BSc Honors degree in IT (Sp. Cyber Security)

Introduction to Cyber Security - IE2022

Table of Contents

1. Abstract

The swift expansion of Internet of Things (IOT) has incorporated new security challenges and vulnerabilities in systems. Apart from all the attacks available, Man-in-the-Middle (MitM) attack is so prominent because of its nature as it could be a passive or active attack. These attacks could take place due to an unauthorized entity which intercepts and potentially alters communication between the IOT devices, which could lead to system breaches, data leaks and unauthorized access to sensitive information. With the available constraints in IOT devices, the old traditional security mechanisms such as complex cryptographic algorithms may be infeasible due to the lightweight in the present solutions.

This report describes how MITM attacks function throughout the network, application and physical levels of the IOT architecture, and this paper divides them into passive and active attacks. Some of the examples for real-world examples are Verkada camera hack in 2021 and Equifax data breach in 2017, elaborate the catastrophic consequences of MITM exploits. [1] Moreover, this research highlights attack techniques like IP spoofing, and DNS spoofing play in jeopardizing IOT networks.

Protocol-based defenses such as Domain Name System Security Extensions (DNSSEC) and Transport Layer Security/Diagnostic Trouble Codes (TLS/DTCS), and intrusion detection systems (IDS) techniques for identifying anomalies are among the current mitigation measures that are carefully reviewed. The lack of common security standards, such as resource limitations of IOT devices, and difficulty of detecting dynamic attacks are only a few of the major issues that exist.

Future research directions, enhanced machine learning models, and controlling a robust IOT ecosystem are all included in the report's summary. One of the promising direction is self-healing networks that can autonomously detect and neutralize MITM threats. It helps create strong, scalable defenses against MITM attacks in IOT by applying the information that already exists and identifying the gaps, guaranteeing safe and reliable smart systems in the future.

2. Introduction

The Internet of Things (IoT) is evolving with technology by interacting with billions of devices ranging from sensors to applications across homes, cities and industries. Even if Internet of Things is efficient and convenient, its rapid expansion has led to serious security and privacy issues, with Man-in-the-Middle (MitM) attacks being one of the most dangerous threat to IoT systems. According to statistics over 40 billion IoT devices are predicted to be connected globally by 2030. [1] Man-in-the-middle attacks are very dangerous because it could be an active or a passive attack depending on the attacker's motive.

A man-in-the-middle attack occurs when an unauthorized party modifies or monitors a data in a network. Most of the Internet of Things devices are built using simple operating systems and low power components to maintain its simplicity and, in the meantime, it limits their capacity to incorporate modern security features. Man-in-the-Middle attacks are very prominent in IoT devices because of numerous characteristics, which includes of unencrypted communication, analytics mention that 98 percent of IoT traffic is unsecured [1] due to weak authentication, outdated firmware, default passwords and the computing limitations of devices.

This report focuses on investigating methods to identify and mitigate man-in-the-middle attacks in IoT environments. Moreover, emphasizing on the best practices of frameworks, including the National Institute of Standards and Technology's (NIST) Cybersecurity for IoT program, IoT security maturity Model, and the Open Worldwide Application Security Project's (OWASP) guidelines [2], it offers a broad analysis of system vulnerabilities present in IoT systems. Also it is important to consider using adaptive authentication protocols, secure booting procedures and frequent firmware updates. Below figure shows the general overview of how a man-in-the-middle attack take place.

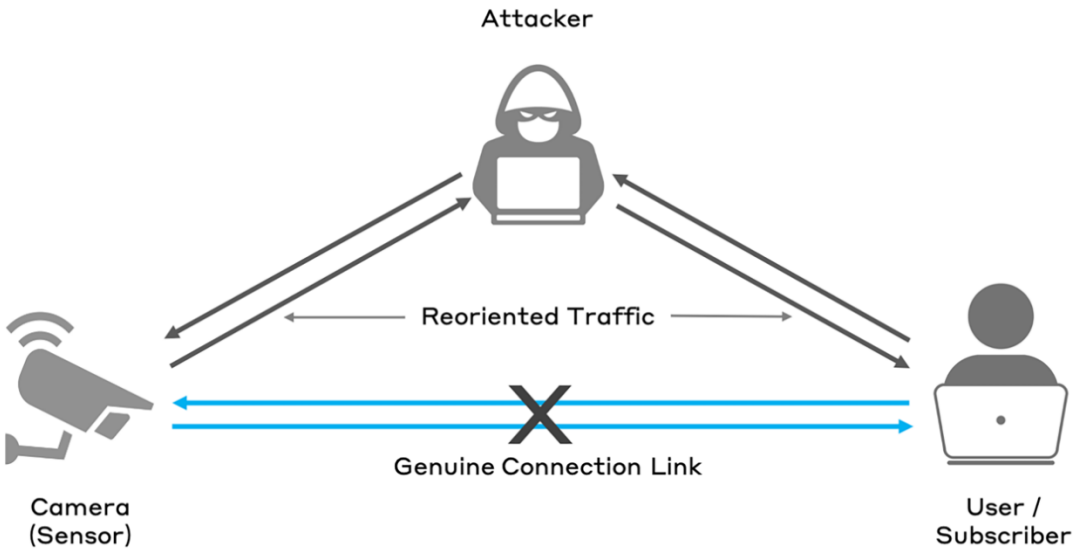

Figure 1- A general schema of man-in-the-middle attack. [1]

The research also highlights the need of security by design principles in development stage, for example manufacturers might have bear a cost ahead of security, and mainly in large scale productions. Protection from MitM attacks is very important as the use of IoT spreads into delicate industries like transportation, healthcare, engineering and also in military.

This study provides insight on how to improve the security on devices connected to internet and provides the basis of mitigating man-in-the-middle attacks over the internet.

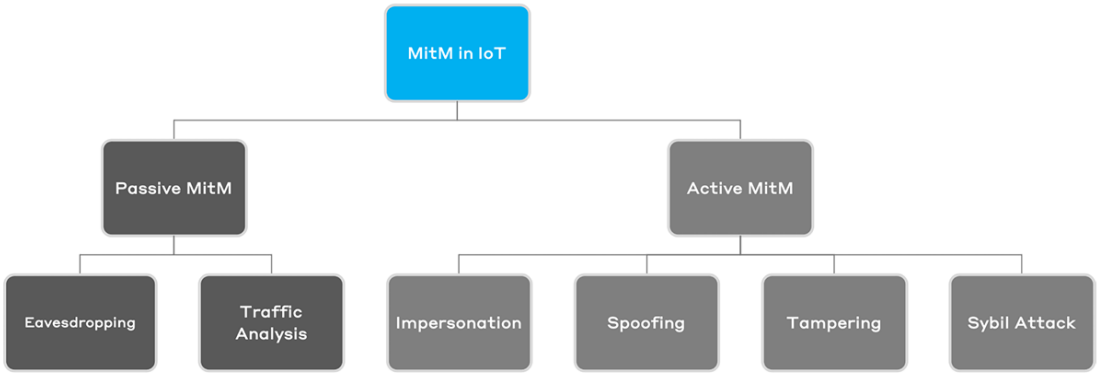

Figure 2- Passive and active man-in-the-middle attacks. [1]

3. Evolution to the topic

The mitigation of man-in-the-middle attacks has evolved rapidly due to increase in threats and expansion of technology. In the early days risks were fairly straightforward because most of the devices used basic protocols for communication. By taking advantage of open ports or default credentials, most attacks were eavesdropping on the networks. By then most of the networks used hypertext transfer protocol (HTTP) which were not so secure. In this stage main focus was to develop affordable and functional IoT devices. Most of the devices were designed with minimal processing power and security wasn't focused much. [3]

With the expansion of wireless IoT devices, most of the devices were connected to Wi-Fi, Bluetooth and other low powered networks. Due to this it also led to more sophisticated network exploits, including address poisoning and session hijacking. Network layer vulnerabilities such as unsecured Message Queuing Telemetry Transport (MQTT) protocols. This led to the reliance of weak access control in MitM attacks, also it doesn't only intercept data but also alters it. In 2021, from analytics it has been discovered that 16 out of 20 popular smart home appliances were vulnerable to MitM attacks due its poor encryption, unlock doors, or outdated communication protocols. [4]

With the integration of IoT into cloud infrastructure, attack scope shifted to remote device management, cloud-based commands and centralized data streams. While hypertext transfer protocol Secured (HTTPS)become the main channel. Also in this stage vulnerabilities in manipulating state data, camera streams and accessing logs could be done anywhere in the world.The advent of AI-driven Advanced persistent threats (APTs) increased the complexity. AI- based bots and malware are now capable of learning the device behavior and understand the traffic and disrupt the service. Additionally, researchers are exploring quantum-resistant algorithms and AI-powered anomaly detection for early threat detection and mitigation.

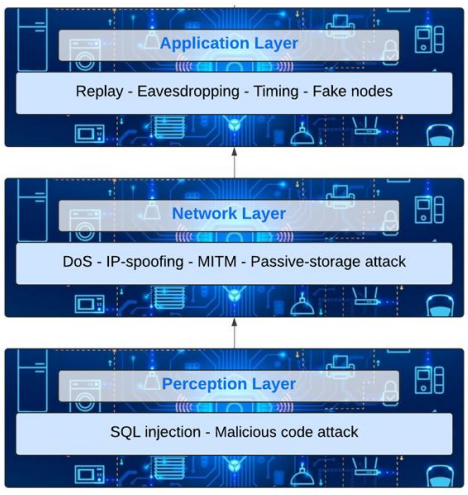

Figure 3 - IoT attacks across layers [11]

A. Early IOT Risks and Simple Eavesdropping

In the early stages of Internet of Things (IoT), the focus was largely on device affordability and functionality. Due to that security was often neglected or considered afterthought. One of the most prevalent threat during this time was simple eavesdropping, it is a basic form of man-in-the-middle attack where data transmission between IoT devices and their controllers could be intercepted and read.

Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT), or raw TCP without any encryption were commonly used in past for IoT devices to communicate to each other. A 2023 study by Al Kabir et al. discovered that up to 98% of IoT traffic being sent without any security precautions. [3] Since its open nature it made it easier for hackers to obtain login credentials, user commands, and activity tracking. Smart home products like door locks and cameras are in high danger due to its privacy issues.

Furthermore, illegal access was possible with little effort because a large number of IoT devices were shipped with default passwords and unprotected ports. Ahmed et al.'s 2024 study also showed that a badly designed communication interface and a lack of authentication made it simple for attackers to alter data streams and control traffic. [5]

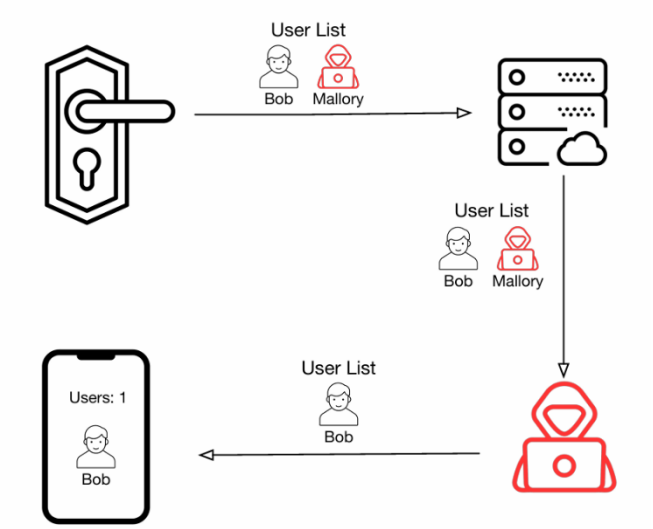

Figure 4 - Attackers can also leverage man-in-the-middle at tacks to spoof response messages carrying user lists or de vice histories. [4]

B. Development of Network Exploits and Wireless IoT

The development of wireless Internet of Things (IoT) systems has introduced a new pathway for automation, connectivity of infrastructure. However, this expansion has also led to increase in network vulnerabilities. A Man-in-the-Middle (MitM) attack happens when a malevolent actor, monitor or modifies communication between two endpoints. Due to the open and accessible nature of wireless IoT communication, there is a greater chance of such attacks in wireless IoT devices.

Lightweight wireless communication technologies like Bluetooth smart, Zigbee and Wi-Fi are frequently used by IoT devices. Since these protocols weren't originally designed with robust security features, attacks find them to be appealing targets. For instance, Zigbee doesn't always have a strong encryption, Bluetooth smart can be vulnerable for unauthorized pairing. These threats are exploited through network-based attacks like replay attacks, session hijacking and eavesdropping, which act the base for man-in-the-middle attacks.

A hypothetical scenario involves an attacker setting an access point to impersonate a legitimate network. When a user connects a IoT device to this network, attackers would be able to take control over to the device and manipulate the data. This would lead to critical issues such as data leaks or unauthorized control of smart home appliances.

To mitigate these risks, a strong encryption to IoT appliances should be implemented with proper authentication protocols. Moreover, regular system updates and implementing an intrusion detection system (IDS) would help to capture and reduce the MitM attacks. Studying how these network exploits are created is very important, therefore developing proper IoT architecture that is resistant to emerging threats would reduce the risk of MitM attacks. The below figure 4 shows IoT architecture layers from networking perspective, perception layer contains the sensors and controlling devices that act as the physical environment. IoT protocols can be categorized into four logical layers as follows.

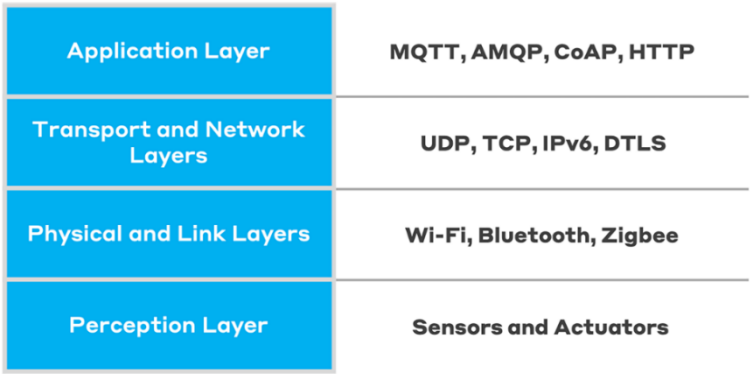

Figure 5 - IoT network architecture layers. [1] [13]

C. Advanced Attacks on IoT Connected to the Cloud

The union of Internet of Things and cloud computing have joined hands to produce scalable and efficient solutions, in healthcare, transportation, and smart home. But the surface for the malicious attackers grew as well through this union. The man-in-the-middle attack is a dangerous vector in this sense because it becomes even more advanced when IoT devices are connected with the cloud. Cloud based for data transfer, analytics, and firmware update, IoT devices are dependent on the cloud platforms' constant connectivity. Wireless networks and lightweight protocols like MQTT, and HTTP, which do not have robust security, are generally used for these transfers.

Attackers can take advantage of the reality that over 98 percent of IoT traffic is still unsecured by positioning themselves between the device and the cloud to steal, tamper with, or inject malicious commands. In addition to compromising the CIA trinity of confidentiality, integrity, and availability, these attacks have the potential to physically destroy real-world systems, particularly key infrastructure like smart grids or healthcare systems. [1]

These types of cyberattacks like MitM are growing more advanced as IoT finds its way into cloud environments as quickly as it is. They need to be addressed by an end-to-end architectural redesign with maximum priority being on security-by-design, real-time monitoring, and secure communication protocols. They can no longer be considered standalone threats. The maximum potential of IoT in cloud environments will never become a reality without proactive security.

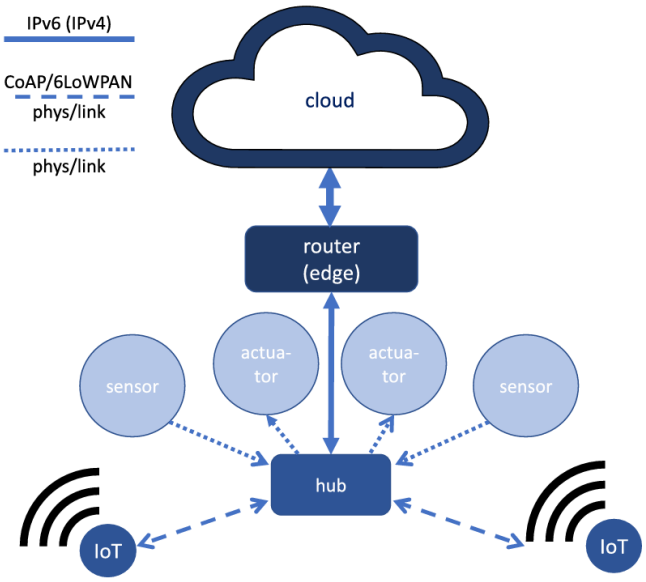

Figure 6 - Deployment architecture of IoT networks and their integration. [13]

IoT networks leverage cloud platforms for:

- Data storage and analytics
- Remote configuration and updates
- Synchronization of devices across devices
- Control logic and user interface

These features necessitate ongoing data exchange, typically over wireless media, between IoT devices and cloud servers. As soon as attackers can use MitM attacks to intercept, manipulate, or forge messages, this arrangement is vulnerable, particularly when endpoint validation, authentication, or encryption is missing or insufficient.

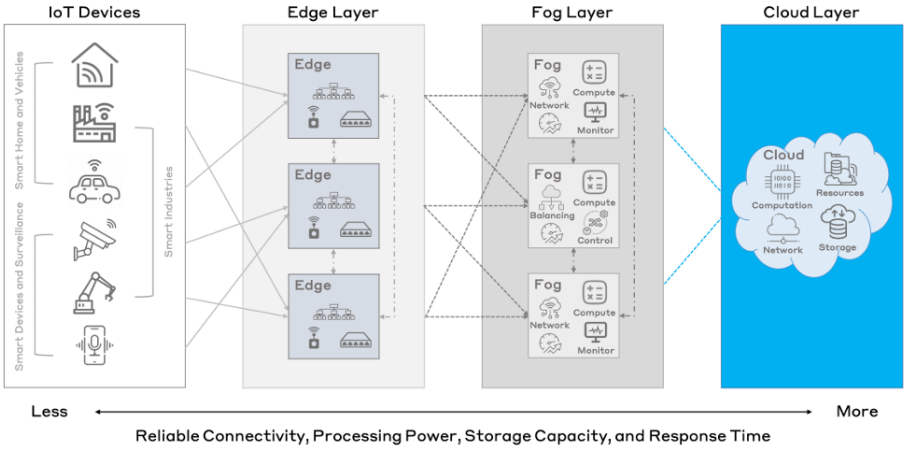

Figure 7 - A general view of IoT infrastructure. [1]

D. Advanced Persistent Threats Powered with AI

Man-in-the-Middle (MitM) attacks within Internet of Things (IoT) networks have taken a new turn with the emergence of Advanced Persistent Threats (APTs), which is a type of cyberattack characterized by stealth, persistence, and intelligent targeting. With the integration of artificial intelligence (AI), APTs can be launched in an adaptive, dynamic, and destructive manner, particularly in wireless and cloud-based Internet of Things networks.

AI-driven APTs utilize machine learning processes to:

- Monitor network traffic to avoid detection
- Automatically identify hijacked cloud gateways and Internet of Things devices
- Adapt their attack strategies in real time based on the behavior of their environment.

These intrusions can steal information, change the behavior of a device, or launch a large, coordinated attack without being detected for a long time. Attackers utilize AI models to duplicate legitimate traffic in a bid to evade intrusion detection systems by infiltrating lightweight protocols like MQTT or Constrained Application Protocol (CoAP) in the Internet of Things.

Artificial intelligence-powered Advanced Persistent Threats (APTs) are a malevolent evolution of cyber attacks, particularly in Internet of Things networked systems. Using machine learning, future-generation attacks can enumerate vulnerable devices, search through network traffic independently, and adapt their strategy in real time to remain stealthy. [6] With protocols like MQTT and CoAP that are light in weight, AI-powered APTs infiltrate IoT networks. The attacks, designed to resemble normal device communication, can silently compromise systems in the long run. Using them, hackers can carry out sustained, stealthy attacks in which they can control the device behavior, exfiltrate confidential data, or lay the foundation for an extended network compromise.

The agility of AI-powered APTs redefines the cybersecurity landscape of IoT networks. The attacks are particularly resilient since, unlike typical attacks, they use reinforcement learning to continuously optimize their attack strategy in terms of protecting the network. [7] An AI-powered APT, for instance, can first infect a single smart sensor, after which it utilizes generative adversarial networks to learn and copy normal patterns of traffic in the network while it attacks horizontally. [8] AI-APTs pose the greatest risk in smart city and industrial IoT deployments due to their capacity for learning and evolving, and can cause disruption.

E. Security Measures Resistant towards AI and Quantum

with the latest technologies i.e. IoT devices are becoming more entrenched in critical infrastructure and day-to-day life, it has never been more important to have better security against dynamic threats, and most importantly Man-in-the-Middle (MitM) threats. The cybersecurity landscape is transforming with developments in AI-driven attacks and threats leering with the onset of quantum computers to break conventional encryption. All of this is propelling development further and further propelling the effort to put new physical security systems in place that resist attacks that are magnified by AI or quantum computing, the latest breakthrough in MitM technologies for IoT prevention and mitigation.

AI, potentially interpreted as being defensive in nature, is being misused by hackers in the guise of automated and higher-order types of MitM attacks. When applied to IoT devices as they often communicate over insecure or very lightweight protocols, the impact can be significant and can last for an indeterminate amount of time without being detected. Quantum computing creates an additional threat landscape. Quantum computers like Shor's and Grover's could make every existing encryption method obsolete, allowing data collected during a MitM attack to be decoded within seconds once

In response to both threats, the establishment of Post-Quantum Cryptography (PQC) is now a necessity. PQC algorithms - CRYSTALS-Kyber and Dilithium - that are approved by NIST, yield quantum-sound encryption schemes regardless of how quantum decryption methods are applied. [9] Such encryptions standards are paramount for the security of communication taking place between IoT devices, especially with MitM threats using broadened attack tactics against weak, old, or obsolete cryptographic protocols.

At the same time, AI is being used more defensively. Machine learning software trained on collections of, or patterns of network traffic flow can detect anomalies or possible MitM and allow actions to be taken to stop the attacks in real time. Further, when combined with zero trust architecture (ZTA), in which everything - communication, and access requests - are authenticated at all times, the potential for intrusion by satisfaction, or laterally moving into an IoT network is reduced. [10] The operation of AI detection, post-quantum cryptography and zero trust architecture represent is the culmination of the actual history of prevention against MitM attack, moving from , quantum-computer safe, and AI-based methodological protection.

The integration of AI-based detection, post-quantum crypto, and zero trust will not only provide better security for IoT, but it will ultimately provide immunity to cyberattacks - even the most sophisticated ones. As we complete the embedding of MitM mitigation into IoT ecosystems, we should realize that future-proofing our defense fundamentally rests on the innovation future threats.

4. Future developments

As IoT networks become larger and more complex, the focus of future advancements in cybersecurity is shifting to the development of intelligent, decentralized, and quantum-resistant infrastructures. One of the main components of focus is the deployment of Artificial Intelligence-based Intrusion Detection Systems (IDS) that can respond to MitM attacks in real time by evaluating traffic patterns and anomalies with machine learning algorithms. Research confirms that AI-assisted IDS can sufficiently decrease false event accuracies and apprehend advanced attacks that elude traditional solutions. [10]

Simultaneously, Quantum-Resistant Cryptography is becoming a critical defense against next-generation quantum enabled decryption attacks. CRYSTALS-Kyber and Dilithium, among other algorithms are being tested to see if they can protect IoT communications even under attack by a quantum-enabled attacker. [9] Such encryption methods will be necessary in keeping data confidential for longer time spans, as IoT devices itself become increasingly connected.

An additional promising avenue of study is the use of blockchain-based decentralized security protocols that remove single points of failure by distributing authentication and data validation through a secure and immutable ledger. Blockchain has been demonstrated to prevent spoofing as well as unauthorized data interception in IoT systems. [11]

Moreover, there are key management systems that have post-quantum cryptography, and will be better supporting end-to-end encryption. These technologies have strong key safeguarding features, as this is typically the weakest link in MitM attacks. Last, the advent of edge computing and 5G technologies will change the landscape of IoT security. Because edge computing allows data to be processed closer to the data's source, the decrease in physical distance carries potential benefits such as reduced latency and reduced network attack possibilities, while 5G's greatest draw is its increased speeds and security; both an advantage to all of us.

All of these future efforts, and efforts to come, are breaking the mold of building an extremely resilient IoT system for preventing today and the future's cybersecurity breach.

A. AI-Powered Intrusion Detection Systems for Preventing MITM Attacks in IOT Networks

As IoT devices are incorporated into increasingly vital systems like healthcare, homes, and infrastructure, they can also be attractive point of targets for cyber hackers in general and Man-in-the-Middle (MitM) attacks in particular. Both the security measures and attacks have a delay, as security measures can never move as fast as they need to match the rapidly changing, decentralized nature of IoT environments which leaves the networks exposed to increasingly sophisticated intrusion attempts. In such cases, AI-based Intrusion Detection Systems (IDS) can also be used as an effective solution to proactively identify and combat MitM attacks.

AI-based IDS employ machine learning approaches to examine large amounts of network traffic data in real-time. Once they learn the "normal" behavior of a network's devices and streams of communication, they can detect relatively slight changes that might signal an active MitM attack, for example: unexpected changes in source IP address, latency, unauthorized copying of data, among others. AI and ML-based IDS systems can detect data security incidents that "signature-based system" relying on known attack signatures cannot, and are potentially more adaptable to new and recently identified attack methods.

For instance, supervised models are possible to use for the classification of a network event based upon labeled data, whereas uses of unsupervised models (for example- clustering or anomaly detection) for the detection of unknown patterns will rely on prior disclosed knowledge. Deep learning-based structures such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) are being used to efficiently process temporal and spatial patterns in IoT traffic. For such tech exhibited an increase detection capabilities for MitM activities by the system's characters to low-end equipment, etc.

A report done by Bhardwaj et al. found that AI-assisted security frameworks for IoT networks are becoming more important in enhancing the real-time detection of threats with fewer false positives. AI-IDS is the next step in addressing the ever-evolving MitM attacks in protecting IoT networks of the future where smart, automated defense will react faster and more accurately than any human eye can monitor independently. [10]

B. Quantum-Resistant Cryptography for Securing IoT Communications.

With the raging progress of quantum computing, industries are concerned with the future of their current cryptographic algorithms, especially those securing Internet of Things (IoT) communication. Conventional encryption systems such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) rely on the difficulty of problems such as prime factorization and discrete logarithms, problems which can be solved by quantum algorithms like Shor's algorithm with immense efficiency, that's the current scary power of quantum computing. Disruption due to this possible endeavor will make Post-Quantum Cryptography or Quantum-Resistant Cryptography vital to protect IoT networks from imminent Man-in-the-Middle (MitM) attacks.

IoT devices operate in resource-constrained environments and communicate sensitive data over open networks, making them highly vulnerable to interception and tampering. The emergence of the quantum computer will put even intercepted encrypted data at risk, as it will eventually be possible to reverse the encryption and show private messages. PQC is an effort to establish a portion of cryptographic algorithms that are quantum-resilient, while also being efficient enough to run on IoT devices.

The National Institute of Standards and Technology (NIST) has taken the lead in standardizing post-quantum algorithms around the globe. Algorithms such as CRYSTALS-Kyber for encryption for digital signatures emerged as pre-eminent candidates based on quantum resistance and performance.

For IoT, the use of quantum-resistant cryptographic protocols ensures long-term data confidentiality, integrity, and authenticity. According to Chen et al in 2022, Post-Quantum Cryptography (PQC) should be provided from the beginning of the designs for next-generation IoT systems because most IoT devices have long lifetimes, and will also be vulnerable to cyber-attacks that have the potential to change the landscape. As we anticipate an era with quantum technology concerns, preparing IoT networks for future quantum-safe communication protocols should not be an upgrade in strategy, but rather an evolution in defending against future MitM attacks. [12]

C. Blockchain-Based Decentralized Security Protocols for IOT Networks.

Increasingly, as the number of devices connecting to networks grow with complexity and interrelatedness, centralized security designs failed to keep up with the speed, scale and diversity of devices. Centralized organizations can create single points of failure, as well as latency which can both be leveraged as potential focus points for a Man-in-the-Middle (MitM) attack. Due to these potential vulnerabilities, we are witnessing an increasing percentage of experts examine blockchain-based decentralized security protocols as a very favorable option for securing IoT networks.

Blockchain is, by definition, a distributed, tamper evident ledger that enables trustless communication between devices. In IoT implementations, blockchain enables devices to confirm and share data with one another while not trusting a third party. This significantly reduces the chances of malicious actors intercepting communications. Each transaction or data transfer is encrypted and cryptographically signed and then placed in a block. The block is confirmed by a group of nodes on the network to make it virtually impossible for attackers to spoof device-to-device communications, which is critical protection against MitM attacks.

Another aspect of smart contracts, which are self-executing code stored on the blockchain, is its ability to enforce security policies autonomously, including validating device identities, access control, and identifying anomalies. Recently included are lightweight blockchain protocols such as IOTA and Hyperledger Fabric, which were focused on being lightweight for IoT applications from the outset. These platforms provide a means to transfer information securely between peer nodes, and in a real-time manner without engaging in intermediaries (example -centralized authorities). They also pave the way toward energy-efficient and scalable approaches to security.

In general, implementations of blockchain to IoT security provide a decentralized, verifiable, and tamper-proof solution that mitigates not only MitM attacks, but also makes IoT ecosystem more trustworthy and autonomous.

D. Secure Key Management and Post-Quantum Cryptography in IOT Systems.

The secure management of keys is fundamental to IoT security in terms of keeping communication between devices confidential and ensuring its integrity. Most IoT devices are typically operating in untrusted and decentralized environments, and if the key used to secure the communication with another device is either exposed or poorly managed, or compromised, the risk of Man-in-the-Middle (MitM) attacks is significantly higher. Typical key management and distribution mechanisms (example- public key infrastructures (PKIs)) may not scale with the ubiquitous and uncontrolled proliferation of IoT devices, particularly when devices have limited processing capabilities and memory.

To solve these limitations, researchers are incorporating Post-Quantum Cryptography (PQC) into key management designs, such that future deployments are quantum-aided attack-proof. Future universal quantum computers will be able to break many of the widely used cryptographic schemes like RSA and ECC, leaving the existing key exchange and authentication mechanisms vulnerable to attacks. PQC schemes based on lattice-based problems, or multivariate equations are mathematically sound alternatives that exist as secure against classical and quantum threat models.

One of the areas of innovation focuses on lightweight key exchange mechanisms that use quantum resistant algorithms, such as CRYSTAL-Kyber, proposed by NIST for standardization. These approaches offer low-latency, compact encryption for resource constrained IoT environments. Also, key management mechanisms and key rotation methods with period round key, push the envelope in limiting exposure of sensitive data even if there is a partial compromise.

The continued proliferation of IoT devices places strong key management and quantum-secure cryptographic algorithms at the center of security guarantees for future communication security and compromised system integrity.

E. Edge Computing and 5G to Improve IoT Security and Reduce MITM Attacks

Edge Computing and 5G are working together to help secure the evolving attack surface of next generation Internet of Things (IoT) networks, by increasing the capacity for real-time processing and decreasing latency on IoT networks. As a result, IoT networks will be more resistant and resilient to MitM attacks in terms of distance-based eavesdropping and tampering.

Edge computing is the processing of data closer to the source of the data (example - at or near the IoT device itself) instead of bringing all the data back to a centralized cloud server to process. Because less data has to traverse faraway networks, the attack surface is greatly reduced in terms of data being intercepted and unauthorized access to the data being exposed. Edge processing of data also enables faster threat detection and threat response. Quick response times are crucial when for mitigation and response to MitM attacks.

The capabilities of 5G networks, with high bandwidth and ultra-low latency, further enhance this security model of real-time encrypted communications. 5G network slicing allows the creation of separate virtual networks with unique security, which can provide protection for specific IoT applications designed for highly secure environments.

Key benefits include:

- Less latency provides quicker response times.
- Decentralized processing reduces exposure to outside attack vectors.
- 5G secure communication enhances encryption possibilities.
- Isolation errors can prevent malware and breaches from spreading to other devices.

Providing computing at the edge and securing the communication backbone, Edge and 5G technologies also significantly reduce exposure to MitM attacks in future IoT systems.

5. Conclusion

As the Internet of Things (IoT) extends into critical areas, the risk posed by Man-in-the-Middle (MitM) attacks increases at the same rate. Existing security controls are inadequate to protect against the new and advanced methods of exploitation utilized by attackers. This paper has explored some original solutions that all share the same intent of forming a safer IoT security framework. From smart, AI-based intrusion detection systems that provide real-time threat awareness, to quantum-resistant cryptographic protocols that provide long-term confidentiality, the IoT security future will involve smart, adaptive, and resilient technologies.

Decentralized security technology (like blockchain) not only removes single points of failure and establishes trustless communication; it also enables secure key management systems that leverage quantum safe authentication techniques (they will continue Quantum-Safe Event Stream Data Fabric Security APIs) to prevent security or breach events even in the presence of quantum capability. Finally, as much as edge computing will offer many benefits, including less latency through 5G infrastructure causing quicker reaction time to deal with threats and will lower the chance of being intercepted because processing is closer to where the data is created.

Taken together, these advances indicate not just incremental advances but a necessary step in protecting IoT systems against current and future M-M attacks. As these technologies develop and interact, they open up the path to an intelligent, autonomous, and secure IoT ecosystem—one that can withstand the cyber rigors of tomorrow.

6. References

[1] O. F. M. Z. Hamidreza Fereidouni, "Wiley online LIbrary," 05 Match 2025. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/spy2.70016.

[2] OWASP Foundation, Inc., "Owasp," OWASP Foundation, Inc., 2024. [Online]. Available: https://owasp.org/www-project-internet-of-things/. [Accessed 18 April 2025].

[3] W. E. ,. M. S. S. Mohammed Aziz Al Kabir, "Taylor & fancis online," 12 july 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23742917.2023.2228053#abstract. [Accessed 20 April 2025].

[4] D. C. D. J. TJ OConnor, "ACM Digitial Library," 07 september 2021. [Online]. Available: https://dl.acm.org/doi/10.1145/3474718.3474729. [Accessed 17 April 2025].

[5] Z. I. S. U. M. O. N. W. &. A. M. Ahmad, "Kashf Journal of Multidisciplinary Research," 2024. [Online]. Available: https://kjmr.com.pk/kjmr. [Accessed 18 April 2025].

[6] A. D. O. M. B. C. A. R. Colin Topping, "science Direct," 7 May 2021. [Online]. Available: https://pdf.sciencedirectassets.com/271887/1-s2.0-S0167404821X00077/1-s2.0-S0167404821001486/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEF0aCXVzLWVhc3QtMSJIMEYCIQDMlQWRSjbpzXMURtiCUhZc83U2lDRf8q%2FY7kfcRd4O3AIhAK2ICRAytTEE3n0i5orteDXyfgBuPm0DsgGeOyrikM. [Accessed 20 April 2025].

[7] M. D. ,. L. C. ,. P. B. Adam N Joinson, "Journal of Cyber Sercurity," 19 April 2023. [Online]. Available: https://academic.oup.com/cybersecurity/article/9/1/tyad007/7130095. [Accessed 20 April 2025].

[8] M. B. S. A. J. C. H. T. P. Eckersley, "cornell University," february 2018. [Online]. Available: https://arxiv.org/pdf/1802.07228. [Accessed 20 April 2025].

[9] S. J. Y.-K. L. D. M. R. P. R. P. D. S.-T. Lily Chen, April 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf. [Accessed 20 April 2025].

[10] P. D. P. C. Arvind Kumar Bhardwaj, 20 August 2024. [Online]. Available: https://mesopotamian.press/journals/index.php/BJML/article/view/487/354. [Accessed 20 April 2025].

[11] A. A. Seetah Almarri, "MDPI," 21 November 2024. [Online]. Available: https://www.mdpi.com/2071-1050/16/23/10177. [Accessed 20 April 2025].

[12] L. D. T. P. P. S. Erdem Alkim, "Cryptology ePrint Archive," 10 July 2019. [Online]. Available: https://eprint.iacr.org/2015/1092.pdf. [Accessed 20 April 2025].

[13] D. Trek, "IEEE Xplore," 21 April 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9406023. [Accessed 20 April 2025].