Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Enhanced Multi-Factor Authentication framework to increase the attack detection speed in Intrusion Detection System

V.V.S.R.Kethan Kumar, S. Yogeeswar, Ch. Bhargavi, Dr. B. Annapurna, P. Goyal Kumar, Dr. M. Madhusudhan subramanyam

Department of Computer Science

and Engineering,

Koneru Lakshmaiah Education Foundation,

Vaddeswaram, Andhra Pradesh, India

Abstract Recognizing the rapid growth of the Internet of Things highlights the urgent need for strong security measures, especially with the number of IoT devices expected to reach 75.44 billion by 2025. Despite advancements in security techniques like ethical hacking and machine learning, IoT-specific vulnerabilities persist, necessitating innovative approaches such as Bug Bounty Programs and Responsible Disclosure. The effectiveness of these strategies remains uncertain, emphasizing the importance of comprehensive security planning tailored to the dynamic IoT landscape. MITM attacks leverage advanced encryption, blockchain, and Enhanced Multi-Factor Authentication (E-MFA). The framework proposes post-quantum cryptography, blockchain integration for decentralized key management, and advanced biometrics for user authentication. Machine learning aids in anomaly detection for threat mitigation. The architectural design includes intrusion detection, SSL encryption, and firewalls, emphasizing continuous monitoring and incident response planning to enhance MITM attack detection speed and performance.

Keywords—Internet of Things, Enhanced Multi-Factor Authentication (E-MFA), Intrusion Detection Systems, MITM attacks, Vulnerabilities, Post-Quantum Cryptography, Blockchain Technology

1. Introduction

1.1 The Landscape of IoT Security

An overview of the integration of IoT with daily life and the ensuing difficulties in guaranteeing security, safety, and reliability are given in this section. The exponential growth in the number of IoT devices, projected to reach 75.44 billion by 2025, raises concerns about security vulnerabilities. The focus is on cyber-physical risks compromising confidentiality, integrity, availability, and authentication in IoT applications.

1.2 Challenges and Strategies in IoT Security

Addressing the security concerns associated with the vast number of IOT devices, this section explores the difficulties in implementing strong security measures due to limited resources. Vulnerabilities are used by cybercriminals, which results in data breaches and cyberattacks. Discussions are held on topics including threat detection with machine learning, penetration testing, vulnerability assessment, and ethical hacking. Despite advancements, businesses struggle with unique IoT vulnerabilities, prompting researchers to investigate crowdsourcing security techniques like Responsible Disclosure and Bug Bounty Programs.

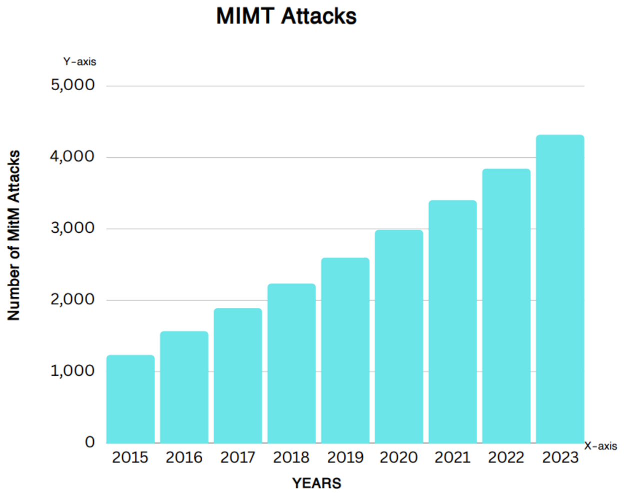

Fig. 1. MITM Attacks Analysis

1.3 Evaluating IoT Security Strategies

In this final section, the focus shifts to the importance of researching and evaluating emerging strategies for IoT security, such as Responsible Disclosure and Bug Bounty Programs. The lack of comprehensive research on their adoption and effectiveness in the IoT space is highlighted, emphasizing the need for a thorough plan considering the nuances of various applications and evolving attack techniques. The subsequent sections aim to provide stakeholders with insights and recommendations to navigate the rapidly changing technological landscape and strengthen IoT security. Fig. 1.

II. Literature Review

Kousik Barik et al. [1] study blends blockchain using ai to improve customer happiness in the context of online buying. It uses enhanced k means and c-means clusteringas well as LSTM networks, to evaluate consumer sentiment with great accuracy and efficiency. Its shortcomings include relying on a single dataset, failing to address all factors influencing blockchain adoption, and failing to address the technical features of blockchain platforms. The limitations in this methodology it exemplifies the major advantages of combining blockchain with AI in the field of gauging customer satisfaction.

K. Fizza et al., [2] Discusses the crucial role of IoT in gathering and processing data from remote locations but points out issues related to power constraints affecting data encryption and device authentication. The paper focuses on exploring security risks in IoT, but drawbacks include repetitive mentions of budget constraints and a limited discussion on potential security solutions.

M. Bhardwaj, [3] underscores the significance of firmware in IoT devices and the reliance on third-party components (TPCs), emphasizing security concerns. The study analyzes 34,136 firmware images, revealing 584 TPCs leading to 128,757 vulnerabilities. However, drawbacks include a lack of proposed solutions and the complexity of findings, suggesting a need for a more concise presentation for improved accessibility.

B. Zhao et al., [4] explores the use of the Internet of Medical Things (IoMT) to address challenges in traditional healthcare systems but notes vulnerabilities, including security and privacy gaps. Emphasizing the need for robust security measures and training, it reviews IoMT's issues and assesses cryptographic solutions. It proposes a multi-layered security approach but acknowledges challenges with zero-day attacks, lacking explicit strategies for mitigation.

J.-P. A. Yaacoub et al., [5] The text discusses the integration of the KEEN module in a Unix/Linux tools course, aiming to foster an entrepreneurial mindset and address technical objectives. It explores ethical hacking's importance in information security. While the survey indicates positive impacts on students, it identifies room for improvement in ethics action plan development. The abstract lacks explicit mitigation strategies for this improvement and may benefit from a more nuanced presentation to avoid potential repetition across iterations.

S. S. Shetty, R. R. Shetty, T. G. Shetty, and D. J. D'Souza, [6] The growing challenge of data security amid increased internet users and web applications, emphasizing the importance of regular security testing, specifically Vulnerability Assessment and Penetration Testing (VAPT). However, potential drawbacks include a lack of specific examples for practical application and an emphasis on VAPT over alternative security strategies, possibly limiting the breadth of considerations.

R. Dvorak, H. Dillon, N. Ralston, and J. Welch,. [7] The critical challenge of ensuring website security amid the exponential growth of internet usage. It introduces Vulnerability Assessment and Penetration Testing (VAPT) as complementary techniques for analyzing and addressing website vulnerabilities. However, the abstract lacks specific examples or elaboration on the challenges in website security, and further details on the distinctions between VAPT techniques could enhance reader understanding.

G. Krasniqi and V. Bejtullahu, [8] The rise of cyber attacks and the adoption of anti-forensics techniques by cyber-criminals, leading to increased attack sophistication. Traditional security measures are considered insufficient, necessitating the development of advanced forensic tools. Drawbacks include a potential lack of specific examples and detailed solutions to counter threats, as well as the absence of explicit proposals for advanced forensic tools or strategies.

S. Atul Hassan, [9] The rise of cyber attacks on IoT domains, emphasizing the sophistication of cyber-criminals using anti-forensics to evade detection. Traditional security and forensics measures are considered inadequate, necessitating advanced forensic techniques. The paper reviews various forensics and anti-forensics methods in the IoT domain, aiming to equip investigators with insights into cyber-criminals' methodologies. Drawbacks include a potential lack of specific examples and detailed solutions, as well as the absence of explicit proposals for advanced forensic tools or strategies, limiting practical guidance.

J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab,. [10] The growing concern for IoT security in the face of increased incidents and vulnerabilities. It proposes practical guidelines for addressing these challenges and explores the use of Bug Bounty Programs (BBP) and Responsible Disclosure (RD) as crowdsource ethical hacking approaches. Using qualitative investigation methods, including literature surveys and expert interviews. Drawbacks include a potential lack of quantitative analysis and the need for specific examples to enhance understanding and practical applicability.

III. State Of Art

3.1 Advancements in Encryption and Blockchain Integration

In this segment, the research explores a multifaceted approach to address contemporary Man-in-the-Middle (MITM) attacks. The focus is on leveraging cutting-edge encryption standard, to fortify data integrity and confidentiality. The proposal advocates for the adoption of advanced encryption techniques to mitigate vulnerabilities in communication channels. Additionally, it is spoken of using blockchain technology to improve certificate authorities' and key management's security, promoting a decentralized and tamper-resistant foundation for secure communications.

3.2 Enhanced Multi-Factor Authentication and AI-driven Anomaly Detection

This section delves into the second facet of the proposed strategy, emphasizing user authentication and real-time threat detection. Enhanced Multi-Factor Authentication (E-MFA), particularly incorporating advanced biometrics, is recommended to bolster user authentication processes. Furthermore, the research suggests harnessing the power of AI and ML for real-time anomaly detection in network traffic. This approach aims to enable early identification and mitigation of potential MITM threats, contributing to a proactive defense strategy. In an ever-evolving cyber threat scenario, the conversation also emphasizes the significance of constant monitoring, incident response planning, and compliance with industry standards as fundamental components of the all-encompassing framework to counter MITM assaults. Case studies and simulations provide practical insights, demonstrating the efficacy of the proposed strategy, while the discussion of challenges and future directions aims to guide ongoing efforts in cybersecurity research and development.

3.3 Objectives

3.3.1 To frame an efficient tool to increase the detection speed of MITM attack.

3.3.2 To increase the performance of the toll to reduce the MITM attacks.

IV. ARCHITECTURAL DESIGN

It mainly focuses on three areas of security mechanisms

4.1 Intrusion detection

Intrusion detection is a security mechanism aimed at identifying and responding to unauthorized or malicious activities within a computer system or network. It works by continuously monitoring and analyzing network or system events to spot potential security threats. The objective is to quickly detect unusual patterns or behaviors that may signal a security breach. Intrusion detection systems employ various techniques, such as signature-based detection, anomaly detection, and behavioral analysis, to strengthen security and reduce the likelihood of unauthorized access or cyberattacks. Continuous monitoring and real-time alerts are crucial elements of successful intrusion detection strategies.

4.2 SSL Encryption

SSL encryption, or Secure Socket Layer, is a cryptographic protocol used to secure data transmission over a network. It employs a combination of public and private key encryption to establish a secure and encrypted connection between a user's web browser and the server. SSL ensures data integrity, confidentiality, and authenticity, safeguarding sensitive information such as login credentials or financial transactions. With advancements like TLS (Transport Layer Security), SSL is widely used to create a secure communication channel on the internet, providing a crucial layer of protection against eavesdropping and data tampering. The efficacy of SSL encryption must be preserved by regular upgrades and adherence to security best practices.

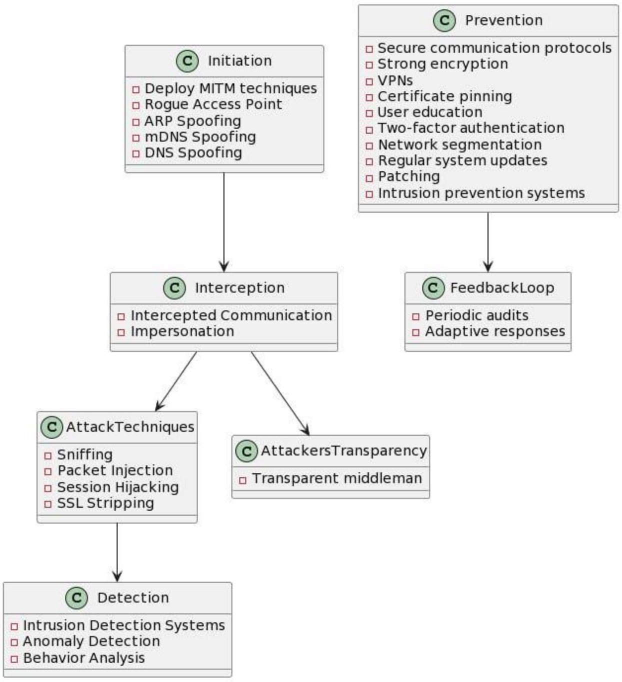

Fig. 2 MITM System Order

4.3 Firewalls

Incoming and outgoing network traffic is monitored and controlled by firewalls, which operate as a barrier between trusted internal networks and untrusted external networks. They operate based on predetermined security rules to permit or block data packets, enhancing overall network security. Firewalls can be hardware or software-based, with the former typically deployed at network boundaries and the latter on individual devices. They are essential in limiting the possibility of criminal activity, guarding against cyberattacks, and blocking unwanted access. Regular updates to firewall rules and configurations are essential to adapt to evolving cybersecurity threats and maintain robust protection.

It also regulate network traffic based on specified security rules, enforcing policies to block or allow data packets. They operate at various layers, such as network, transport, or application layer, providing comprehensive protection. Stateful inspection, a common firewall technique, monitors the state of active connections, allowing or denying traffic based on context. For increased security, next-generation firewalls include sophisticated capabilities including application-layer filtering, deep packet inspection, and intrusion prevention. A layered security solution must include firewalls in addition to other security measures like IDS and antivirus software. Regular monitoring, updates, and customization of firewall settings are essential to adapt to emerging threats and maintain an effective defense posture. Fig. 2. Explains about the connections between these sections represent their interactions within the overall system.

V. System Methodology

5.1 MITM Attack Methodology for Data Theft

Intercepted Communication: Intercepted data between two parties, making them believe they were communicating directly. Impersonation: Positioned as a middleman, impersonating parties to eavesdrop or manipulate data. Attacker's Transparency: Remained unseen, acting as a transparent middleman during data exchange.

Attack Scenarios and Techniques: Employed Rogue Access Point, ARP Spoofing, DNS Spoofing, DNS Spoofing. Utilized MITM Techniques: Sniffing, Packet Injection, Session Hijacking, SSL Stripping.

5.2 Detection

Detecting MITM attacks is challenging due to their covert nature. To identify odd patterns, make use of behavior analysis, anomaly detection, and intrusion detection systems. Keep an eye out for irregularities in network traffic and utilize instruments that detect unwanted access or rerouting. Update and patch systems often to address security holes that might be exploited by MITM attackers. Conduct periodic security audits and implement real-time monitoring to quickly detect and respond to suspicious activities.

5.3 Prevention

Prevent MITM attacks by using secure communication protocols like HTTPS. Implement strong encryption methods and enforce the use of virtual private networks (VPNs) for sensitive data transmission. Employ certificate pinning to verify the authenticity of SSL/TLS certificates. Educate users about phishing risks and encourage the use of two-factor authentication. Employ network segmentation to limit the impact of potential attacks. Regularly update and patch systems to close known vulnerabilities. Analyze network traffic for abnormal patterns and utilize intrusion prevention systems to detect and prevent Man-in-the-Middle (MITM) attacks.

Vi. Experimental Results

The speed at which a vulnerability detection tool can identify and report security vulnerabilities is a critical factor in its effectiveness. A faster tool can help security teams to identify and remediate vulnerabilities more quickly, reducing the risk of a successful attack.

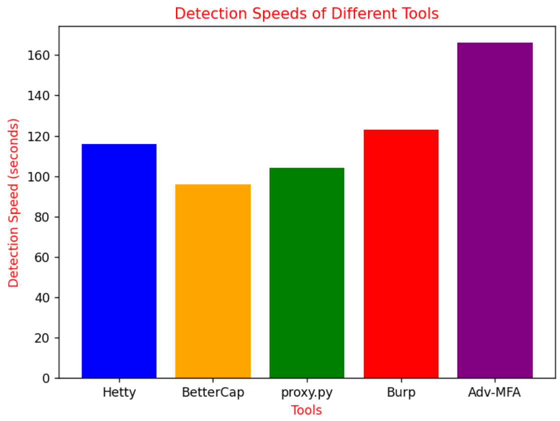

Fig. 3. Detection Speeds of Different Tools

Our experiment and Fig. 3. support that our hypothesis that Adv-MFA is the fastest vulnerability detection tool. It was able to detect vulnerabilities more quickly than the other four tools. However, it is important to note that the detection speed of a tool is just one factor to consider when choosing a tool for detecting vulnerabilities and security issues. Other factors to consider include the accuracy of the tool, the ease of use of tool, and the cost of the tool.

VII. Conclusion & Future Work

Our research unveils a comprehensive strategy for combating Man-in-the-Middle,(MITM) attacks are becoming more common in today's cyber threat scenario. Leveraging advanced encryption, blockchain integration, and Enhanced Multi-Factor Authentication, our proposed framework exhibited notable efficacy in reducing vulnerabilities in communication channels. The case studies and simulations provided practical insights, affirming the viability of our approach.

Moving forward, our focus shifts towards refining the MITM detection tool for enhanced speed and performance. Real-world implementation challenges will be addressed, ensuring seamless integration into diverse environments.

References

[1] [1]“Effect of Spectrum Prediction on Cognitive Radio Networks,” Spectrum Sharing in Cognitive Radio Networks, pp. 77–96, Jun. 2021, doi: 10.1002/9781119665458.ch4.

[2] K. Fizza et al., “QoE in IoT: a vision, survey and future directions,” Discover Internet of Things, vol. 1, no. 1, Feb. 2021, doi: 10.1007/s43926-021-00006-7.

[3] M. Bhardwaj, “Research on IoT Governance, Security, and Privacy Issues of Internet of Things,” Privacy Vulnerabilities and Data Security Challenges in the IoT, pp. 115–134, Oct. 2020, doi: 10.1201/9780429322969-7.

[4] B. Zhao et al., “A large-scale empirical analysis of the vulnerabilities introduced by third-party components in IoT firmware,” Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, Jul. 2022, doi: 10.1145/3533767.3534366.

[5] J.-P. A. Yaacoub et al., “Securing internet of medical things systems: Limitations, issues and recommendations,” Future Generation Computer Systems, vol. 105, pp. 581–606, Apr. 2020, doi: 10.1016/j.future.2019.12.028.

[6] S. S. Shetty, R. R. Shetty, T. G. Shetty, and D. J. D’Souza, “Survey of hacking techniques and it’s prevention,” 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Sep. 2017, doi: 10.1109/icpcsi.2017.8392053.

[7] R. Dvorak, H. Dillon, N. Ralston, and J. Welch, “Exploring Ethical Hacking from Multiple Viewpoints,” 2020 ASEE Virtual Annual Conference Content Access Proceedings, doi: 10.18260/1-2--34640.

[8] G. Krasniqi and V. Bejtullahu, “Vulnerability Assessment and Penetration Testing: Case study on web application security,” 2018 UBT International Conference, Oct. 2018, doi: 10.33107/ubt-ic.2018.213.

[9] S. tul Hassan, “Analysis of Vulnerabilities in System by Penetration Testing,” Pakistan Journal of Scientific Research, vol. 2, no. 1, pp. 22–25, Jun. 2022, doi: 10.57041/pjosr.v2i1.23.

[10] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, “Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations,” Internet of Things, vol. 19, p. 100544, Aug. 2022, doi: 10.1016/j.iot.2022.100544.

[11] I. Hafeez, A. Y. Ding, S. Tarkoma. 2017. IOTURVA: Securing Device-to-Device (D2D) Communication in IoT Networks. In Proceedings of the 12th ACM MobiCom Workshop on Challenged Networks (CHANTS '17)

[12] A. Schrottenloher and M. Stevens, “Simplified Modeling of MITM Attacks for Block Ciphers: New (Quantum) Attacks,” IACR Transactions on Symmetric Cryptology, pp. 146–183, Sep. 2023, doi: 10.46586/tosc.v2023.i3.146-183.

[13] L. Rahman, “Detecting MITM Based on Challenge Request Protocol,” 2015 IEEE 39th Annual Computer Software and Applications Conference, Jul. 2015, doi: 10.1109/compsac.2015.135.

[14] E. Welbourne et al., “Building the Internet of Things Using RFID: The RFID Ecosystem Experience,” IEEE Internet Computing, vol. 13, no. 3, pp. 48–55, May 2009, doi: 10.1109/mic.2009.52.

[15] S. Z. DİCLE, “Man-In-The-Middle Attack,” European Journal of Science and Technology, Oct. 2022, doi: 10.31590/ejosat.1187984.

[16] W.-L. Chen and Q. Wu, “A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal,” Proceedings of the Asia-Pacific Advanced Network, vol. 30, no. 0, p. 66, Dec. 2010, doi: 10.7125/apan.30.10.

[17] Y. J. Ham and H.-W. Lee, “Vulnerability analysis on Mobile VoIP supplementary services and MITM attack,” 2013 International Computer Science and Engineering Conference (ICSEC), Sep. 2013, doi: 10.1109/icsec.2013.6694815.

[18] A. Sebbar, M. Boulmalf, M. Dafir Ech-Cherif El Kettani, and Y. Baddi, “Detection MITM Attack in Multi-SDN Controller,” 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), Oct. 2018, doi: 10.1109/cist.2018.8596479.

[19] B. I. Bakare and S. M. Ekolama, “Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls,” European Journal of Electrical Engineering and Computer Science, vol. 5, no. 4, pp. 63–68, Aug. 2021, doi: 10.24018/ejece.2021.5.4.336.

[20] U. O. Obonna et al., “Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms,” Future Internet, vol. 15, no. 8, p. 280, Aug. 2023, doi: 10.3390/fi15080280.