Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Delve into the architecture of defensive strategies to protect IoT devices from targeted attacks

Mohammed Rajih Mohammed*

University of Al-Qadisisya, Collage of Biotechnology, Iraq.Email: mohammed.rajih@qu.edu.iq

ARTICLE INFO

Article history:
Received: 25 /04/2025
Rrevised form: 11/06/2025
Accepted : 25/06/2025
Available online: 30/06/2025

Keywords:

cyber-attacks,

IoT,

protect interconnected systems,
security assessment

ABSTRACT

The great development in information technology and the Internet of Things is accompanied by several concerns, the most important of which are security vulnerabilities and cyber-attacks that affect the joints of the connection between resources, as old methods are no longer sufficient to reduce security vulnerabilities and protect interconnected systems.

The study aimed to design a strategy that works on defense, combating deception, controlling operating systems, and diversity in the process of operational mobility with a process of updating and evaluating in real time by deploying deceptive nodes and dynamically moving between operating systems of Internet of Things devices and continuously monitoring the attack surface.

This study focuses on the security returns resulting from the designed system, as it adopts a multi-layered security approach to protect Internet of Things networks from complex and targeted threats. This defensive approach is a powerful approach to increase the complexity of attackers and try to stop them and improve the overall resilience of the Internet of Things ecosystem. The effectiveness of the proposed defense-in-depth strategy is evaluated through simulation and performance analysis, which indicates its ability to mitigate various types of attacks while maintaining acceptable overhead.

https://doi.org/10.29304/jqcsm.2025.17.22201

1. Introduction

The increasing adoption of the Internet of Things (IoT) in critical sectors such as healthcare, manufacturing and transportation has led to a significant increase in the number of connected devices [1]. While these devices offer improved functionality and convenience, they also have significant security vulnerabilities and IoT landscape expands exponentially and becomes more complete, they become attractive targets for predators. IoT devices transmit sensitive data for as health information, operational metrics, or personal data over the Internet.. End-to-end encryption (E2EE) at the device level, such as a series of communication channels, is essential [2].

Redlining is very important to limit cyber propaganda. The concept of isolation signifies the construction of individual microcircuits to create IoT devices or group devices.. The access control (RBAC), the multi-facturer authentication (MFA) and the limited privileges principles guarantee that the users of the automated systems can interact with the IoT intelligent devices.. Outdated firmware or software is an exploitable vulnerability in IoT

∗Corresponding author: Mohammed Rajih Mohammed

Email addresses: *mohammed.rajih@qu.edu.iq*

Communicated by 'sub etitor'

devices. Regular updates and security patches are needed to overcome vulnerabilities [3]. Automated update and security mechanisms reduce the possibility of hackers attacking devices without parts. The IoT monitor continues to detect unusual activities or people that may help identify them and mitigate the risks they may cause before they cause major losses. Intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with automatic learning-based anomaly detection tools, can alert administrators about erratic behavior [4].

It is important to build IoT devices and repair the device to remove unnecessary services that attackers may explore, as well as setting security systems and establishing hardware arrangements [3-7]. Additionally, it is important to have cryptographic protocols to mitigate potential risks. It is highly demanded to prioritize Malware, DoS attacks, and physical tampering among which the Internet of Things (IoT) may be subject to security breaches [3]. It is essential to arrange a clear incident response plan that includes detection, removal, and recovery steps to minimizing the impact of a cyber-attack.

The rapid growth of Internet of Things (IoT) devices across industries has exposed serious security issues. These devices are exposed to various risks including distributed denial of service (DDoS) attacks, malware infections, and data breaches [8].

It is insufficient to focus on security issues with a single cover to defend against full attacks from different stages considering complicated connection of IoT devices., Defense-in-depth (DiD) techniques have been applied to stop these threats. Several security methods are included to reduce the risks of targeted attacks [9]. IoT devices, especially those with limited resources such as processing power, memory, and power, are interested in the list and the ability to support advanced security protocols [7, 8, 10].

This makes them particularly vulnerable to cyber-attacks. Furthermore, the reliance of many IoT applications on real-time means that any interruption in the availability of red data can lead to catastrophic consequences, especially in sectors such as medical attention and transportation [11]. A defense-in-depth strategy involves implementing several security mechanisms, each designed to prevent or mitigate different types of attacks [12].

Physical access to devices must be restricted, especially for critical systems in healthcare, manufacturing, or smart infrastructure, and dividing the IoT network into parts based on function or security level has isolated compromised devices [13]. Red splitting prevents attackers from easily positioning themselves horizontally between devices. Monitoring red traffic while scanning for unusual customers can help detect attack episodes. Intrusion detection systems (IDS) can identify potential threats, while intrusion prevention systems (IPS) effectively prevent malicious activity [14, 15].

Objectives of the Study

Evaluate the effectiveness of different security layers according to the defense-in-depth strategy in protecting IoT devices from targeted attacks and evaluate the efficiency of each security layer individually and jointly and using statistical tables and performance metrics. for Analyze the results.

Related Work

Multi-layered defense strategies efficiently helps enhancing the security of Internet of Things (IoT) devices against targeted attacks [16]. Ensuring comprehensive protection against diverse threats is gained by applying a set of integrated security strategies . This study aims to revise the latest research on multi-layered defense strategies for IoT devices.

It is efficient to introduce diversity and uncertainty into attacks According to Aboelwafa .et al (2020) [17]to initiate mobile attack surfaces for web services. Changing configurations and resources are essential topics to prevent targeted attacks and forces attackers to deal with a high level of uncertainty.

Ahanger .et al (2022) [18] presented an active deception framework to develop environment for adaptive cyber deception. It aims to strengthen defenses against advanced attacks by using dynamic deception techniques.

Ahmad, W., (2022) [19] discusses mobile defense issues using software-defined networks including the use of the technology of random modification of hosts via the OpenFlow network as a mobile. This technology can provide a transparent defense against targeted attacks.

Al-Masri, E. et al (2020) [20] studied random code encryption to immunize targeted attacks. This technology contributes to enhancing application security by hiding and diversifying software configurations.

Additionally, Alyahya, S. (2022) [21] pointed out the importance of improving Internet routing through the principle of Software Defined Networking (SDN). It helps improve traffic management and reduces the risk of targeted attacks.

Furthermore, Applying advanced encryption and anonymity measures mentioned by Bala, B. (2024) [22] who addressed the issue of hiding data flows in 6LoWPAN IoT networks to enhance the security of data transmitted over the network .

In addition, Ben Othman, S., et al (2022) [23] discussed SDN infrastructure protection in IoT networks against Man-in-the-Middle (MitM) attacks where they have proposed ways to prevent network threats targeting communication data.

as Also, proactive defense strategies proposed by Chatterjee, U., and Ray, S. (2022) [24] for the software-defined Internet environment against multi-target attacks are valuable. They focus on improving security considering early detection and rapid response to threats.

Leveraging SDN for Security Deception Liu, Grigoryan, Cho, Y., et al (2022) [25] reviewed how to leverage SDN to improve deception strategies in the Internet of Things. This approach enhances security by using new methods to improve defenses.

Methodology

This methodology defines a multi-layered security approach to protect IoT devices from targeted attacks, combining deception-based deception, moving target defense (MTD) through operating system diversification, and real-time security assessment.

Setting up the network architecture:

The first step in implementing a defense-in-depth strategy is to create an IoT network architecture. This includes determining the network topology and identifying node vulnerabilities.

1. Create an IoT network: The user provides system information, such as the initial network topology and vulnerabilities associated with each node. This data is used to create an end-to-end IoT system model, which includes real nodes, servers, VLANs, and SDN controllers, for demonstration purposes, we assume that the network is designed based on a smart hospital setup, where IoT nodes collect data and transmit it to servers. While medical IoT devices are usually expensive and may not support OS diversity, for this model, all devices are assumed to be OS diversity compatible [26].

Output: The output of this phase is the initial architecture of the IoT network, which forms the basis for deploying security mechanisms in subsequent phases.

Deception-based IoT deployment: To trick attackers and divert their attention from important nodes, rogue nodes are deployed within the network.

2. Deploy the real and fake node: Each real IoT node is paired with a decoy node that mimics the characteristics of the real node but serves no operational purpose beyond deception. These rogue nodes are deployed in Virtual Local Area Networks (VLANs) to lure and mislead attackers, and Nodes are classified based on their attributes: true ($ni.r$), decoy ($ni.d$), resolved ($ni.c$), or critical ($ni.r$). These attributes, along with their associated vulnerabilities, are assigned to each node.

Output: The goal of deploying deception is to mislead attackers, force them to interact with non-critical components of the network, and thus protect core nodes from direct attacks.

Diversifying the operating system through MTD (Moving Target Defense): Operating system (OS) diversification is a proactive security technique within the Moving Target Defense (MTD) framework. By periodically changing the operating system on IoT nodes, the attack surface is dynamically changed, complicating the attacker's efforts [27].

3. Apply OS Diversity: At this stage, the system applies OS Diversification to the IoT nodes, which can be either random or based on node importance. This approach introduces a level of uncertainty to attackers by regularly introducing new vulnerabilities that need to be discovered and exploited, and Random OS Diversity: A percentage of nodes in the network are randomly selected to receive a new OS, and IM-Based OS Diversity: Nodes classified as critical for OS changes are prioritized to enhance their security.

Output: Diversifying the operating system increases the complexity of the attacker's task, reducing the probability of successful attacks by constantly changing the attack surface.

Create attack surface and security models: A key component of a defense-in-depth strategy is real-time security monitoring, which requires mapping the attack surface of an IoT network.

4. Harmful Attack Representation Model (HARM): Security Model Generator automatically creates a HARM model to represent the attack surface of the network. The HARM model consists of two layers:

The upper layer captures reachability information for each node, showing how attackers move through the network, and the bottom layer represents the vulnerabilities of each node, identifying potential attack points, and Purpose: By visualizing attack paths and potential vulnerabilities, the HARM model provides a comprehensive view of a network's security posture, enabling real-time analysis of attacker behavior [21].

Security assessment and monitoring: Continuously assessing network security is crucial to detecting and mitigating attacks. The final phase of the defense-in-depth strategy focuses on monitoring security conditions to ensure the system remains protected.

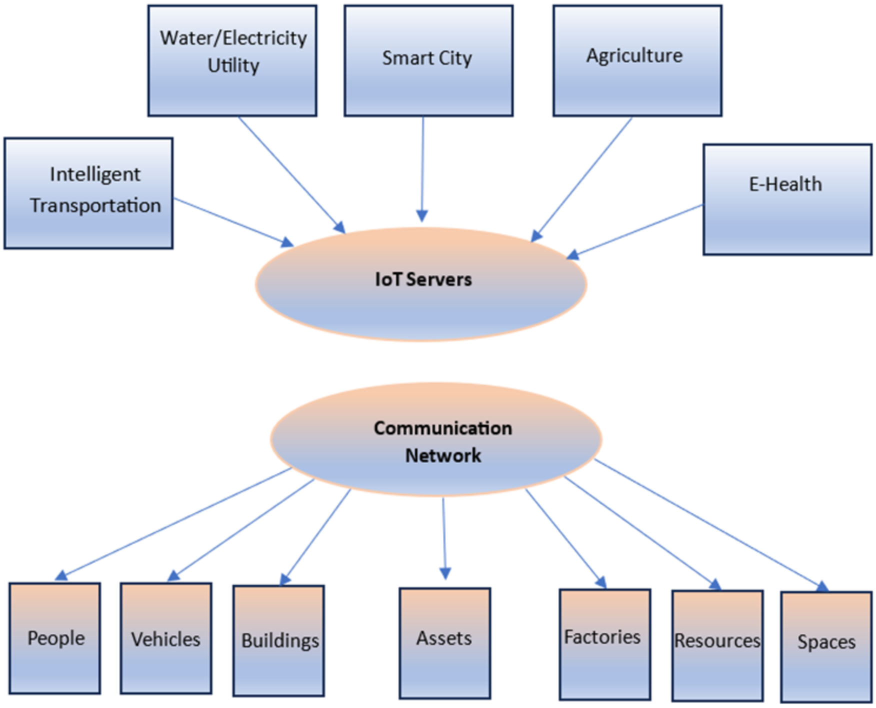

Fig.1 IoT Network Model

5. Ongoing security assessment: Evaluation module leverages the output of the HARM model to evaluate network security using specific conditions:

Loss of Integrity: This occurs when attackers compromise a large portion (e.g., a third) of legitimate nodes through reconnaissance or other attacks and Loss of Confidentiality: This is assessed when sensitive information is leaked to unauthorized entities, either by insiders or external attackers [18].

Output: A continuous security assessment mechanism ensures that the network is constantly monitored for violations, providing early warning signals and enabling immediate remediation.

Basic components of a defense-in-depth strategy

The proposed methodology integrates several key components that work together to provide multi-layered security for IoT devices:

Decoy nodes: These nodes act as decoy elements, diverting attackers from important nodes. Decoys are indistinguishable from real nodes, making attackers more likely to engage. Interacting with booby traps creates alerts for the defender, revealing potential attack vectors and the attacker's intentions, and OS Diversification (MTD): By regularly rotating the operating system on nodes, the network creates new vulnerabilities for attackers to explore. This dynamic attack surface forces attackers to constantly reevaluate their strategies, reducing the effectiveness of static attacks, and Security Monitoring: The HARM model provides a graphical representation of attack paths and vulnerabilities, giving defenders real-time insights into potential threats. Continuous security assessment ensures that any breaches are detected early, minimizing the impact of attacks, and SDN Control: The Software Defined Network (SDN) controller ensures secure communication between IoT nodes and servers, dynamically adjusting traffic flows based on network conditions. This layer adds additional security by managing traffic at a central point [28].

Experimental procedures and Results

Experimental Setup

Secure the devices in a controlled environment to prevent unauthorized physical access, and use security sensors to detect any physical tampering attempts and Configure a firewall to filter incoming and outgoing traffic to and from IoT devices and implement a Virtual Private Network (VPN) to secure communications between devices and the central server and Update the operating systems and firmware on the IoT devices, and disable unnecessary services to minimize potential attack vectors and Install an IDS, such as Snort, to monitor network traffic and detect any suspicious activities and Apply TLS (Transport Layer Security) to all communications between devices, and encrypt stored data using AES-256 (Advanced Encryption Standard) and Software Updates: Set up a server for automatic software updates to ensure that the latest security patches are applied.

Experimental Procedures

Simulate basic attacks without any protection by executing targeted attacks to assess the vulnerability of IoT devices without any security layers, measure the attack success rate and compromised data and implement physical security: Simulate physical attacks on devices to assess the effectiveness of physical security measures, monitor attempts and successes of physical breaches and network security. Activate the firewall and execute attacks such as denial of service (DoS) attacks and man-in-the-middle (MitM) attacks, and evaluate the effectiveness of the firewall in preventing these attacks. Perform data exfiltration. Attacks with encryption enabled and analyze the level of protection of encrypted data. Perform attacks with an IDS in place and evaluate the system’s ability to detect and mitigate threats. Attempt to exploit known vulnerabilities before and after software updates are applied and measure the effectiveness of the updates.

Results

Table.1 summarizes the outcomes of the experiments, showing the success rate of different types of attacks under various security conditions. Additionally, Table.2 summarizes the effectiveness of various protection methods based on their success rates.

Table 1- summarizes the outcomes of the experiments

Security Layer	Type of Attack	Success Rate	Time to Compromise	Data Compromised
No Protection	Exploitation	95%	10 minutes	Unencrypted
Physical Security	Physical Access Attempt	20%	30 minutes	None
Network Security	Man-in-the-Middle Attack	10%	45 minutes	Encrypted
Intrusion Detection	Denial of Service Attack	5%	60 minutes	None
Encryption	Data Exfiltration	0%	-	Unreadable
Software Updates	Exploitation of Vulnerabilities	0%	-	None

Table2 - the effectiveness of various protection methods based on their success rates

Protection Method	Success Rate	Success Rate (%)
No Protection	0.942	94.2
Physical Security	0.209	20.9
Network Security	0.112	11.2
Intrusion Detection	0.061	6.1
Encryption	0.000	0.0
Software Updates	0.000	0.0

Evaluating the Effectiveness of Cybersecurity Countermeasures:

Cyber security is a critical concern for all organizations around the world, as cyber data and data breaches can carry serious consequences in cases of financial loss, due to reputational and standard loyalty issues. This panel displays different success tasks and security methods to protect against different types of cyber threats.

The first series, "Protection from Sin," serves as the norm, indicating that without any security method in place, the success of attacks or breaches is alarmingly high: 94.2%. This brings up the absolute necessity for organizations to implement solid cybersecurity strategies.

Physical security, such as access controls, monitoring systems, and physical barriers, provides a 20.9% success rate in preventing or mitigating attacks. If these methods provide a level of protection, it will only be sufficient if only one fraction of the attacks (79.1%) succeed.

Net Security, including firewalls, intrusion prevention systems, and secure communication protocols, provides up to 11.2% success in protecting against cyber threats. This indicates that red-based security controls can effectively thwart a portion of attacks, but have a better margin to improve the overall security posture of red.

Intrusion detection systems, which monitor red flag traffic and analyze users to identify and respond to unauthorized activity, provide a success rate of up to 6.1% in detecting and preventing intrusions. If not as effective as other methods, intrusion detection systems will provide a crucial foil in the multifaceted focus on cybersecurity.

The table also breaks down the exceptional effectiveness of specific security tools: encryption and software updates. Strategic Ambassadors have a success rate of 0.0%, which indicates that they have great results in protecting against breaches and data attacks. Encryption that codifies confidential data to avoid unauthorized access, and periodic software updating to prevent known vulnerabilities, are essential components of a solid cybersecurity brand.

In conclusion, the data presented indicate the need for organizations to adopt an integrated, multi-capability focus for cybersecurity. If it's only good so you can provide complete protection, the combination of physical security, net security, intrusion detection, code and software updates can significantly improve your overall security posture and reduce the risk of external cyber-attacks.

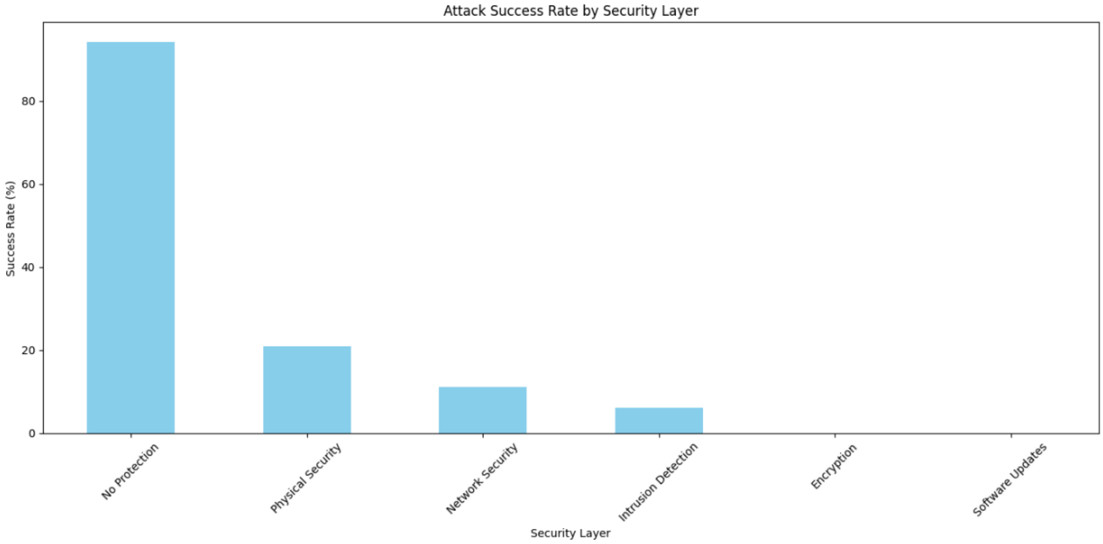

Fig.2 Attack Success Rate by Security Layer

The detailed results provide insight into the success rates of different types of security breaches or attacks. Here's a breakdown of each category:

- Physical Access

Success Rate: 18.3% This indicates that attacks leveraging physical access to systems or facilities have an 18.3% success rate. This suggests that physical security measures may be somewhat effective, but there is still a notable risk of unauthorized access.

- Network Attack

Success Rate: 10.9% Network attacks have a success rate of 10.9%. This relatively low percentage suggests that while network security measures are in place, there is still a vulnerability that can be exploited by attackers.

- IDS Bypass (Intrusion Detection System Bypass)

Success Rate: 4.3% The success rate for bypassing Intrusion Detection Systems (IDS) is only 4.3%. This indicates that IDS are quite effective at detecting and preventing unauthorized access, making it difficult for attackers to succeed using this method.

Data Exfiltration: Success Rate: 0.0% There were no successful data exfiltration attempts recorded, which is a positive outcome. This indicates strong security measures are in place to prevent unauthorized extraction of data.

Vulnerability Exploitation: Success Rate: 0.0% Similar to data exfiltration, there were no successful attempts at exploiting vulnerabilities. This suggests that the systems have been effectively secured against known vulnerabilities.

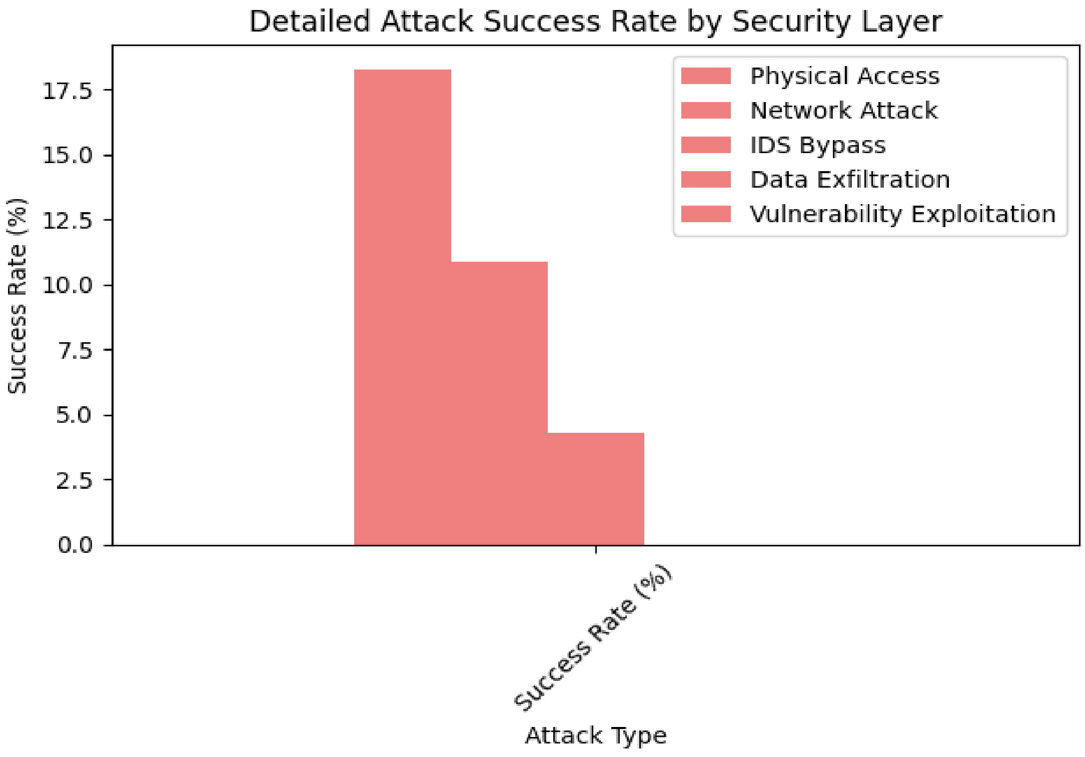

Fig.3 Detailed Attack Success Rate by Security Layer

Analyzing the Synergistic Effects of Multilayered Cybersecurity

Table 3 explores combining different cybersecurity measures and implementing different security controls 1.4% success rate is shown when implementing both physical and network security measures, demonstrating efficient combination of two layers of security. Reduction in the risk of successful attacks is noticed in comparison to to relying on a single layer of a layered approach. Additionally, the success rate of attacks is reduced to 0.0%,which demonstrates the effectiveness of encryption that converts sensitive information into a secure, unreadable format The success rate drops to just 0.1%, demonstrating enhances in the overall security. Intrusion detection systems enable detecting unauthorized activitiesThe All-Layers row shows that when all security measures (physical security, network security, intrusion detection systems, and encryption) are combined, the success rate remains at a constant 0.0%.

Table3 -"Combined Security Layers " in a haiku-inspired format

Security Layers	Success Rate	Success Rate (%)
Physical + Network	0.014	1.4
Physical + Network + IDS	0.001	0.1
Physical + Network + IDS + Encryption	0.000	0.0
All Layers	0.000	0.0

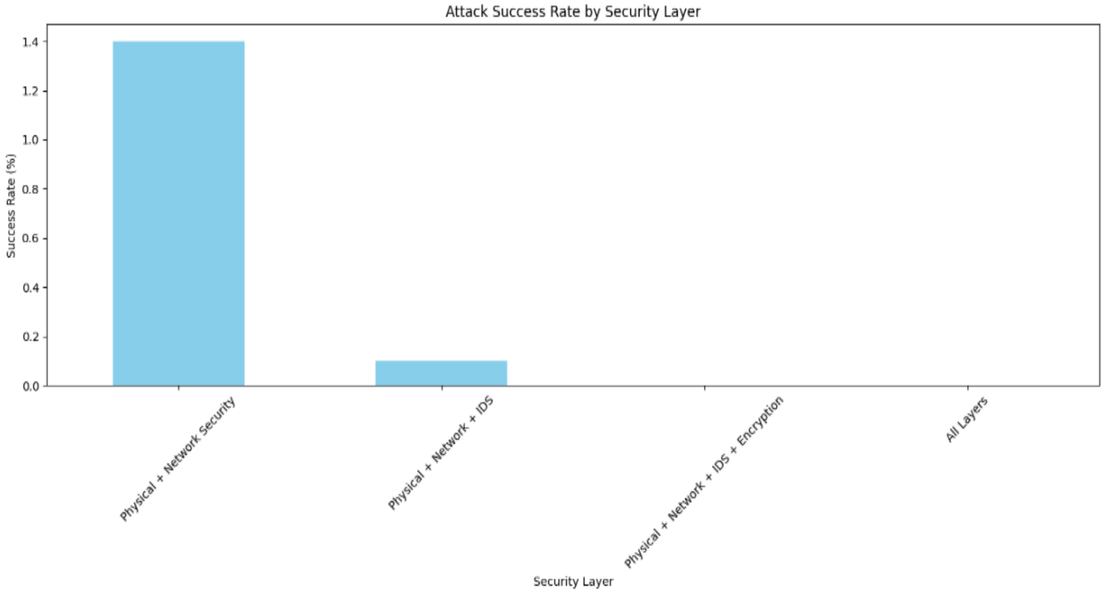

Fig.4 Combined Security Layers

Conclusion*:*

The defense-in-depth strategy presented in this document provides an integrated focus to protect IoT resources from targeted intrusions. By integrating engineered defenses, moving target defense mechanisms, and real-time security monitoring, the methodology provides several protection capabilities that significantly increase attacker completeness. Implementing the following nodes, diversifying the dynamics of the operational system, and continuing to evaluate the work of security teams to detect, repel and dissuade adversaries, reducing the possibility of breaches. Experimental results demonstrate the effectiveness of this depth-focused defense to mitigate various types of attacks, including exploiting vulnerabilities, data leaks, and service violation targets. Multi-level security methods, such as physical security, red-level controls, encryption, and intrusion detection, work together to improve the overall resiliency of the IoT system.

Adopting this defense strategy is especially critical for IoT applications in critical sectors, such as medical attention, manufacturing, and smart infrastructure, where the vulnerability of connected devices could have serious consequences. Despite the unique security challenges that create the IoT ecosystem, they focus on providing a solid mark to protect confidential data and ensure reliable function of core IoT applications. In the future, more research will be needed to explore the potential for escalation and adaptability in a defense-in-depth strategy as IoT trends continue to increase in scale and completeness. Additionally, the integration of emerging technologies, such as artificial intelligence and machine learning, can improve the dynamic and adaptable nature of security methods, allowing for smarter, more proactive defense against evolving cyber threats.

References

[1] Dudhe, P.V., N.V. Kadam, R.M. Hushangabade,M.S. Deshmukh. Internet of Things (IOT): An overview and its applications. in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). 2017. Chennai, India.

[2] Bhuse, V. Review of End-to-End Encryption for Social Media. in Proceedings of the 18th International Conference on Cyber Warfare and Security. 2023. Maryland, USA: Academic Conferences International Limited.

[3] Sodja, C., J. Carroll, M. Turcotte,J. Neil. Automating threat actor tracking: Understanding attacker behavior for intelligence and contextual alerting. 2022 [cited 2024 09/01/2024]; Available from: https://www.microsoft.com/security/blog/automating-threat-actor-tracking/

[4] Dykstra, J., K. Shortridge, J. Met,D. Hough (2022) Sludge for good: Slowing and imposing costs on cyber attackers. arXiv preprint. arXiv:2211.16626. https://doi.org/https://doi.org/10.48550/arXiv.2211.16626

[5] Saeed, S., S.A. Altamimi, N.A. Alkayyal, E. Alshehri,D.A. Alabbad (2023) Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors. 23(15): 6666.

[6] Saeed, S., S.A. Suayyid, M.S. Al-Ghamdi, H. Al-Muhaisen,A.M. Almuhaideb (2023) A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors. 23(16): 7273.

[7] Salzano, A., C.M. Parisi, G. Acampa,M. Nicolella (2023) Existing assets maintenance management: Optimizing maintenance procedures and costs through BIM tools. Automation in Construction. 149: 104788. https://doi.org/https://doi.org/10.1016/j.autcon.2023.104788

[8] Pawlick, J., E. Colbert,Q. Zhu (2019) A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Comput. Surv. 52(4): Article 82. https://doi.org/10.1145/3337772

[9] Zhang, L.,V.L.L. Thing (2021) Three decades of deception techniques in active cyber defense - Retrospect and outlook. Computers & Security. 106: 102288. https://doi.org/https://doi.org/10.1016/j.cose.2021.102288

[10] Vasudevan, V., Z. Zakhour, V. Gomes,S. Raju. Top 10 cybersecurity threats in 2024. 2024 [cited 2024 09/01/2024]; Available from: https://eviden.com/publications/digital-security-magazine/cybersecurity-predictions-2024/top-10-cybersecurity-threats/.

[11] Abolhassani Khajeh, S., M. Saberikamarposhti,A.M. Rahmani (2022) Real-Time Scheduling in IoT Applications: A Systematic Review. Sensors (Basel). 23(1). https://doi.org/10.3390/s23010232

[12] Smith, C.L. Understanding concepts in the defence in depth strategy. in IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings. 2003. Taipei, Taiwan.

[13] Liebowitz, D., S. Nepal, K. Moore, C.J. Christopher, S.S. Kanhere, D. Nguyen, R.C. Timmer, M. Longland,K. Rathakumar. Deception for Cyber Defence: Challenges and Opportunities. in 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). 2021. Atlanta, GA, USA: IEEE.

[14] Mohan, P.V., S. Dixit, A. Gyaneshwar, U. Chadha, K. Srinivasan,J.T. Seo (2022) Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions. Sensors (Basel). 22(6). https://doi.org/10.3390/s22062194

[15] Ahmad, R., I. Alsmadi, W. Alhamdani,L.a. Tawalbeh (2023) Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 56(10): 10733-10811. https://doi.org/10.1007/s10462-023-10437-z

[16] Sheibani, M., S. Konur, I. Awan,A. Qureshi (2024) A Multi-Layered Defence Strategy against DDoS Attacks in SDN/NFV-Based 5G Mobile Networks. Electronics. 13(8): 1515.

[17] Aboelwafa, M.M.N., K.G. Seddik, M.H. Eldefrawy, Y. Gadallah,M. Gidlund (2020) A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. IEEE Internet of Things Journal. 7(9): 8462-8471. https://doi.org/10.1109/JIOT.2020.2991693

[18] Ahanger, T.A., U. Tariq, A. Ibrahim, I. Ullah, Y. Bouteraa,F. Gebali (2022) Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective. Mathematics. 10(8): 1298.

[19] Ahmad, W., A. Rasool, A.R. Javed, T. Baker,Z. Jalil (2022) Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics. 11(1): 16.

[20] Al-Masri, E., K.R. Kalyanam, J. Batts, J. Kim, S. Singh, T. Vo,C. Yan (2020) Investigating Messaging Protocols for the Internet of Things (IoT). IEEE Access. 8: 94880-94911. https://doi.org/10.1109/ACCESS.2020.2993363

[21] Alyahya, S., W.U. Khan, S. Ahmed, S.N.K. Marwat,S. Habib (2022) Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices. Electronics. 11(6): 963.

[22] Bala, B.,S. Behal (2024) AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer Science Review. 52: 100631. https://doi.org/https://doi.org/10.1016/j.cosrev.2024.100631

[23] Ben Othman, S., F.A. Almalki,H. Sakli (2022) Internet of Things in the Healthcare Applications: Overview of Security and Privacy Issues. In Intelligent Healthcare: Infrastructure, Algorithms and Management, Chakraborty, C.,Khosravi, M.R. (eds). Springer Nature Singapore. Singapore

[24] Chatterjee, U.,S. Ray (2022) Security Issues on IoT Communication and Evolving Solutions. In Soft Computing in Interdisciplinary Sciences, Chakraverty, S. (eds). Springer Singapore. Singapore

[25] Cho, Y., J. Oh, D. Kwon, S. Son, J. Lee,Y. Park (2022) A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF. IEEE Access. 10: 101330-101346. https://doi.org/10.1109/ACCESS.2022.3208347

[26] Kavak, H., J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore,S. Shetty (2021) Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity. 7(1). https://doi.org/10.1093/cybsec/tyab005

[27] Jing, H.,J. Wang (2022) [Retracted] Detection of DDoS Attack within Industrial IoT Devices Based on Clustering and Graph Structure Features. Security and Communication Networks. 2022(1): 1401683. https://doi.org/https://doi.org/10.1155/2022/1401683

[28] Web of Science. Web of science search. 2024 [cited 2024 09/01/2024]; Available from: https://www.webofscience.com/wos/author/search.