IoT Security Assessment and Mitigation Strategies for Resilient Military Operations

HSC De Silva[1#] and TSS Nilakshi[2]

[1]*General Sir John Kotelawala Defence University, Sri Lanka*
[2]*General Sir John Kotelawala Defence University, Sri Lanka*
[1#] < 39-adc-0035@kdu.ac.lk>

Abstract— *This study examines how military operations are relying more and more on Internet of Things (IoT) technology, which has both advantages and security risks. In order to understand the influence of operational resilience on IoT security risks and vulnerabilities peculiar to military operations, the study identifies and evaluates these issues. Additionally, it tries to spot weaknesses in current assessment practices and frameworks and provide enhanced frameworks specifically designed for resilient military operations. Additionally, while taking into account the necessity for both proactive security measures and reactive incident response skills, the research looks into efficient mitigation techniques to solve IoT security problems in military operations. To gather and analyze qualitative and quantitative data from research papers, data reports, and articles, the study employs a thorough methodology. The findings and discussions will shed light on the IoT security concerns that have been found, the shortcomings of the current evaluation processes, and suggested mitigation tactics. To secure the integrity and effectiveness of military activities, the research emphasizes the significance of improving IoT security in military operations.*

Keywords— **IoT security, Military operations, Operational resilience, Mitigation strategies**

I. INTRODUCTION

The military industry has seen significant change as a result of the Internet of Things (IoT) technology's rapid progress in recent years. Modern military operations now have access to unmatched benefits related to the IoT's seamless integration of interconnected devices, sensors, and systems. The context-setting information in this opening section sets the stage, which also emphasizes the importance of IoT technology in military situations. Additionally, it describes the military's growing reliance on IoT and explains the study's goals and focus.

The way armed forces carry out their objectives and uphold national security has been changed by the integration of IoT technology in military operations. Unmanned aerial vehicles (UAVs), wearable technology, security cameras, and logistics management systems are just a few examples of the massive network of smart devices that can be created simply due to the Internet of Things (IoT), which promotes real-time data interchange and decision-making capacities. IoT has been widely adopted because of its potential to improve military productivity, adaptability, and situational awareness.

Adoption of IoT in military operations improves communication, maintenance prediction, logistical optimization, situational awareness, and training and simulation. IoT devices offer real-time decision-making, effective mission planning, and quick reactions to dynamic battlefield conditions by producing enormous amounts of data. Predictive maintenance improves the preparedness of military assets and decreases downtime. Supply chain operations are optimized by IoT-driven data analytics, and training and simulation are supported by augmented and virtual reality.

IoT brings new, challenging security issues as it permeates more military operations.

Cyberthreats: When IoT devices are interconnected, the attack surface is larger and military networks are more vulnerable to cyberthreats such data breaches, malware infiltration, and denial-of-service assaults. These dangers have the potential to jeopardize vital military data and disrupt operations.

Data Privacy and Integrity: considering that military data is sensitive, strong measures must be taken to protect its privacy and integrity. Data manipulation or unauthorized access can have serious repercussions for national security, putting military operations and strategic planning in danger.

IoT devices are frequently purchased from different vendors, which leads to supply chain risks. The overall security of military systems could be jeopardized by compromised components or malicious firmware.

Lack of Standardization: It is difficult to develop a coherent and reliable security framework since different IoT devices lack established security protocols.

Insider Threats: A key aspect of IoT security continues to be human interaction. Insider threats have the ability to compromise military systems by exploiting flaws, whether on purpose or accidentally.

To preserve the integrity and efficacy of military operations, it is crucial to strike a balance between utilizing the potential of IoT technology and reducing its related dangers in light of these advantages and security challenges.

The growing use of Internet of Things (IoT) technology in military operations add a number of security concerns and weaknesses, though, which could have a big impact on the efficiency and reliability of military operations.

The following are some of the main IoT security concerns and weaknesses particular to military operations:

IoT devices connected to military networks are a possible target for cyber adversaries, resulting in cyberattacks and data breaches. Successful cyberattacks on IoT devices have the potential to compromise the security, integrity, and availability of sensitive data by allowing unauthorized individuals access to vital military data.

In military operations, physical tampering and device authentication are essential since IoT devices may not have strong security measures, making them vulnerable to unauthorized access. IoT devices are vulnerable to eavesdropping and man-in-the-middle attacks because they are deployed in hostile locations and via insecure communication channels. Sensitive data can be compromised as a result of inadequate device authentication and physical manipulation. Strong device authentication and secure communication channels in IoT devices are crucial for reducing these hazards. IoT supply chains and insider threats provide security hazards because they can take advantage of flaws in manufacturing and manufacturing systems. These flaws could allow for the introduction of forged or stolen components into IoT systems for the military. As older systems might not have been developed with IoT security in mind, legacy system integration might also provide compatibility and security difficulties. Additionally, insider attacks might compromise sensitive data or jeopardize operations, making military personnel with access to IoT devices and networks a security risk. IoT device vulnerabilities in the firmware and software can also be used by attackers to take over the target device.

In order to comprehend operational resilience in military IoT environments, one must first understand resilience in the context of military operations and how it relates to the use of IoT technology. Operational resilience is the capacity of military systems and troops to foresee, withstand, adapt to, and recover from shocks, disruptions, or adversary operations while retaining core capabilities and capabilities. Operational resilience in the context of military IoT environments focuses on the ability of military operations to resist and effectively respond to IoT-related obstacles and threats. Threat Awareness, Resilience Planning, Redundancy and Diversity, Real-Time Monitoring, Adaptive Capacity, Incident Response and Recovery, Training and Education, and Integration with Military Doctrine are key concepts in understanding operational resilience in military IoT contexts.

A. *Research objectives and Research Questions*

In order to understand how these risks affect the resiliency and efficacy of military operations, it is important to recognize and analyze the key IoT security risks and vulnerabilities that are specific to military operations. To analyze the shortcomings and shortcomings of the IoT security state of military systems using the current evaluation methodologies and structures, and to provide modified or enhanced frameworks tailored to the unique challenges faced by resilient military operations. And also, To investigate and make recommendations for efficient mitigation strategies and countermeasures for dealing with IoT security issues in military operations, taking into account the necessity for both proactive precautions and reactive incident response capabilities.

B. *Research Questions*

1. What are the main IoT security risks and vulnerabilities that are unique to military operations, and how do they affect the resilience and effectiveness of these operations?
2. What are the major flaws and drawbacks in existing assessment methods and structures for evaluating the IoT security state of military systems, and how can these structures be adapted or improved to effectively address the specific difficulties faced in resilient military operations?
3. What are the best mitigation tactics and countermeasures for IoT security flaws in military operations, taking into consideration the necessity for both preventive measures and reactive incident response capabilities?

II. METHODOLOGY

The introduction, goals, and objectives of the research were stated at the beginning of the first chapter. A qualitative methodological approach was suggested based on the study's correlational nature, data accessibility, and contextual significance through the use of primary and secondary sources. The method will be applied to the data analysis in the subsequent chapter, which will be followed by a discussion of the findings, outcomes, and recommendations.

III. DISCUSSION

The military Internet of things is widely employed in a variety of areas, including smart camps, sites, campuses, transportation, intelligent medical care, and other areas. There are numerous issues that arise when using military Internet of Things technology to meet the demands of various military applications. For instance, there are numerous types of terminal equipment that come in a variety of shapes, sizes, and functions, and different network connecting technologies, such as wired, wireless, Bluetooth, Zigbee, third generation mobile communication, fourth generation mobile communication, fifth generation mobile communication, and satcom.(Li et al., 2020)

- *Mitigation tactics and countermeasures for IoT security flaws in military operations.*

1. *Secure Device Management:*

Implement robust authentication measures to restrict access to IoT devices:
Only authorized users or devices can access the IoT network and its resources thanks to strong authentication. Use MFA (multi-factor authentication) to provide an additional security layer. MFA often combines the user's knowledge (such as a password), possessions (such as a smart card or token), and/or identity (such as biometric information). For IoT devices, avoid using default or weak credentials and impose strict password complexity requirements.

To guarantee that only authorized devices can connect to the network, use device certificates or secure tokens:
Device certificates are cryptographic identifying credentials that allow for secure device identification. Due to their difficulty in forging or breach, they are more secure than conventional passwords. Hardware tokens or smart cards are examples of secure tokens, which add an extra layer of security and can be used in conjunction with other authentication techniques. A valid certificate or token must be presented by a device when it tries to join the network in order to establish its identity and acquire access.

Implement stringent regulations for the registration and deregistration of devices:
For the purpose of registering and administering IoT devices, keep a central repository or database. This enables improved oversight and management. Establish a systematic procedure for network registration and acceptance of new devices. As a result, each device will go through the appropriate security checks before being given access. Create a procedure for de-registering devices that are no longer in use or that have been compromised. Security is maintained by removing illegal or compromised devices from the network.(Bharti et al., 2022)

2. *Security updates on a regular basis and patch management*:

Update IoT device software and firmware frequently to fix known vulnerabilities:
IoT device makers frequently offer firmware and software upgrades that contain security patches to fix flaws found in the devices. Military organizations should keep up with these changes and make sure their equipment is running the most recent, secure firmware and software. Establish a routine or procedure for monitoring for updates from device manufacturers and swiftly installing them on the currently used devices.

Build a streamlined procedure for timely patch and update deployment:
Create a clear patch management procedure that guarantees the prompt distribution of security updates across all IoT devices connected to the military network. To reduce the risk of exploitation, give priority to crucial fixes that address high-severity vulnerabilities. To save time and effort while patching, think about employing centralized management solutions to remotely apply updates to several devices at once.
It's vital to remember that multiple levels of operational relevance and criticality can apply to IoT devices in military operations. Patch management should therefore take into account the effects of any potential disruptions brought on by updating certain equipment. To keep the mission running smoothly while making sure that devices are properly updated, it could occasionally be necessary to temporarily isolate users or take other security precautions.
Additionally, it is crucial to have a clear testing procedure in place before deploying fixes. Some upgrades could cause unanticipated compatibility problems or conflicts with other programs or gadgets. In order to detect any potential negative impacts before deploying patches in a production setting, it is necessary to test patches in a controlled environment.

3. *Intrusion Detection and Prevention Systems (IDPS):*

Use IDPS to quickly identify and stop harmful activity:
Network traffic and system activities are watched for indications of suspicious or malicious activity by intrusion detection systems (IDS). Beyond simple monitoring, intrusion prevention systems (IPS) can actively stop or stop detected threats from infecting the network or devices. Strategically place IDPS sensors throughout the military IoT network to assure complete coverage of vital resources and communication pathways. In order to spot patterns suggestive of cyberthreats like malware, unauthorized access attempts, or suspicious data exfiltration, these

systems scan network packets, logs, and other data.(Tan et al., 2023)

Configure IDPS to warn security staff or automatically react to threats:

IDPS systems can alert security staff or automatically respond to threats, thwarting immediate attacks and minimizing harm from possible invasions. However, as they could obstruct legitimate communication, automatic responses might not be preferred in crucial military operations. Integrating IDPS systems with SIEM, maintaining continuous monitoring and routine updates, and undergoing tweaking and fine-tuning are all necessary to enable effective threat detection. It's also essential for qualified security personnel to actively chase down risks in order to find sophisticated dangers that might elude automated systems. Military organizations can significantly improve their capacity to identify and respond to potential cyber threats by deploying IDPS with real-time threat detection capabilities and configuring suitable automated responses, safeguarding the availability and integrity of IoT-enabled military operations.

- *Importance of Operational Resilience in Mitigating IoT Security Risks.*

Given that security incidents can have serious repercussions, operational resilience is of utmost importance in reducing IoT security risks in military operations. It guarantees mission continuity, adaptability to changing threats, prompt incident response, reduction of vulnerability window, situational awareness, contingency planning, protection of sensitive data and communication, preservation of public trust, minimization of impact on personnel, and alignment with legal requirements and standards. Military organizations can dramatically improve their capacity to preserve sensitive information, maintain efficient operations, and defend against cyber threats by giving operational resilience first priority.

- *RESULT*

Financial investments in IoT security measures and mitigation tactics can be resource-intensive, having detrimental effects such resource-intensiveness, complexity, operational delays, false positives/negatives, and difficulties with regulatory compliance. It's vital to strike a balance between security measures and operational continuity since overly aggressive security measures may result in false positives or false negatives, which could impede military operations.

IoT security evaluations and mitigation techniques have a variety of beneficial effects on mission assurance, cyber defense, and decreased downtime. By shielding secret material against illegal access and potential espionage, these precautions guarantee the continuation and success of crucial military activities. Cyber defenses are strengthened by strong security measures, which makes it more difficult for adversaries to compromise military systems and launch cyberattacks. Effective security assessments and incident response processes reduce operating pauses while promoting cooperation and confidence among allies, partners, and the general public. Long-term cost reductions are achieved through proactive security evaluations that stop expensive data breaches and cyber catastrophes. Strong security measures and resilient IoT systems offer precise situational awareness, safeguard against internal threats, enable flexibility to new threats, and improve the military's reputation and public image. Instilling discipline in the handling of sensitive data, implementing security assessments assures compliance with security standards and legal requirements.

V. RECOMMENDATION

Military organizations should commit enough resources and manpower for security assessments and mitigation efforts in order to reap the benefits of IoT security assessment and mitigation tactics for resilient military operations. To provide thorough security measures and strike a balance between false positives and false negatives, regular security testing and review are essential. Standardization and interoperability encourage each other and lessen complexity. The significance of following security best practices and being vigilant against potential insider threats is reinforced by ongoing training and awareness campaigns. Information sharing between military organizations, business partners, and governmental organizations is encouraged by giving priority to mission-critical assets and adopting a collaborative approach.

Consistent compliance with pertinent rules and standards is ensured by proactive compliance management. In the event of a security problem, real-time incident response drills help to validate response strategies and save downtime. The need of operational resilience and quick recovery is emphasized in security measures to ensure the continuation of military operations. By incorporating security-by-design concepts into the design and acquisition of IoT devices, security is built in from the start. Engaging security professionals and ethical hackers for unbiased evaluations and validation of security solutions increases operational resilience and safeguards sensitive military assets in an environment where security is becoming more complex and interrelated.(Khan et al., 2021)

VI. CONCLUSION

The use of Internet of Things (IoT) technology in military operations has created new opportunities for improved situational awareness, communication, and operational effectiveness. But in addition to its benefits, IoT adoption in the military setting also poses serious security concerns and vulnerabilities that could jeopardize sensitive data and impair crucial operations. In order to address these issues and offer insightful solutions for protecting military IoT deployments, this research has examined IoT security evaluation and mitigation techniques in robust military operations.

In order to address IoT security risks and vulnerabilities, the study underlines the significance of operational resilience and resilience in military operations. It emphasizes the constantly changing nature of cyber dangers and the necessity of constant observation and flexibility in security evaluations. The study criticizes the shortcomings of the current evaluation techniques and suggests improvements such as dynamic risk modeling, integration of threat intelligence, incident simulation, and red teaming exercises. Effective protection of military IoT networks depends on the use of preventative mitigation tactics and countermeasures. The paper makes major contributions to IoT security and military operations, providing military stakeholders with doable security solutions.

The study emphasizes the important role that IoT security evaluation and mitigation play in robust military operations. It adds significant knowledge to the subject of IoT security by highlighting operational resilience, detecting dangers, and suggesting improvements. In order to guarantee the integrity and efficacy of military operations and, ultimately, to protect national security and interests, a proactive and adaptive security approach is essential.

REFERENCESS

Bharti, M., Kumar, R., Saxena, S., & Sharma, V. (2022). 'A Resource-Blockchain Framework for Safeguarding IoT'. Communications in Computer and Information Science, 1544 CCIS. Retrieved from https://doi.org/10.1007/978-981-16-9576-6_9

Butun, I., Osterberg, P. and Song, H. (2020) 'Security of the internet of things: Vulnerabilities, attacks, and countermeasures', IEEE Communications Surveys &amp;amp; Tutorials, 22(1), pp. 616–644. doi:10.1109/comst.2019.2953364.

Johnsen, F.T. et al. (2018) 'Application of IOT in military operations in a Smart City', 2018 International Conference on Military Communications and Information Systems (ICMCIS) [Preprint]. doi:10.1109/icmcis.2018.8398690.

Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). 'On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions'. PeerJ Computer Science, 7. Retrieved from https://doi.org/10.7717/PEERJ-CS.507

Li, X., Pan, W., An, J., & Wan, P. (2020). 'The Application Research on Military Internet of Things'. In 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2020. Retrieved from https://doi.org/10.1109/ICCWAMTIP51612.2020.9317321

Miloslavskaya, N. and Tolstoy, A. (2018) 'Internet of things: Information security challenges and solutions', Cluster Computing, 22(1), pp. 103–119. doi:10.1007/s10586-018-2823-6.

Obaidat, M.A. et al. (2020) 'A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures', Computers, 9(2), p. 44. doi:10.3390/computers9020044.

Park, K.C. and Shin, D.-H. (2016) 'Security Assessment Framework for IOT Service', Telecommunication Systems, 64(1), pp. 193–209. doi:10.1007/s11235-016-0168-0.

Sobb, T.M. and Turnbull, B. (2020) 'Assessment of cyber security implications of new technology integrations into military supply chains', 2020 IEEE Security and Privacy Workshops (SPW) [Preprint]. doi:10.1109/spw50608.2020.00038.

Sobb, T., Turnbull, B. and Moustafa, N. (2020) 'Supply chain 4.0: A survey of cyber security challenges, solutions and Future Directions', Electronics, 9(11), p. 1864. doi:10.3390/electronics9111864.

Tan, K., Yan, W., Zhang, L., Zhang, Y., Yu, K., & Zhang, T. (2023). 'Dynamic open set specific emitter identification via multi-channel reconstructive discriminant network'. IET Radar, Sonar and Navigation, 17(5). Retrieved from https://doi.org/10.1049/rsn2.12380

AUTHOR BIOGRAPHIES

HMSC De Silva is an Undergraduate from Faculty Of Management Social Sciences And Humanities following the Applied Data Science Communication degree at General Sir John Kothalawala Defence University, Sri Lanka. He has completed Primary and Secondary education at C.W.W.Kannnangara Central Collage Mathugama. He did Engineering Technology, Science For Technology and ICT for Advanced Level Examination.

TSS Nilakshi is an undergraduate from Faculty Of Management Social Sciences And Humanities following the Applied Data Science Communication degree at General Sir John Kotelawala Defence University, Sri Lanka. She completed her primary and secondary education at MR/Olcott Model

School and St/Thomas’ Girls’ High School, Matara. She did Combined mathematics, chemistry and Physics for her Advanced Level Examination. She has achieved the Microsoft certified of Azure Data Fundamentals.