Formosa Journal of Science and Technology (FJST)
Vol. 4, No.1, 2025: 349-368

Strengthening Cyber Resilience through IoBT Best Practices: Future Applications

Mohadib[1*], Achmad Farid Widjdi[2], Azhar Fathoni[3], Saddam Rasyidin Al Faruq[4]
Universitas Pamulang
Corresponding Author: Mohadib, dosen01299@unpam.ac.id

A R T I C L E I N F O

Keywords: Artificial Intelligence, Cybersecurity Innovation, Internet of Battlefield Things, Curriculum, Systematic Literature Review

Received : 3, January
Revised : 17, January
Accepted: 31, January

A B S T R A C T

In today's digital era, Internet of Battlefield Things (IoBT) security has become particularly important in ensuring the success of military operations and national security. Through systematic literature observations reviewing publications from 2015 to 2024, this research aims to identify and implement best practices for securing IoBT in state protection, explore potential study topics for future development, and suggest significant IoBT security research topics for researchers. The research results show that developing strong security standards, implementing effective cybersecurity, increasing security awareness, and training, and developing a curriculum are critical to securing IoBT. Additionally, this research also identifies research opportunities that can help implement effective IoBT security strategies and inspire the development of various training curricula. These recommendations will help implement the best IoBT security practices to enhance national security and inspire academic innovation.

ISSN-E: 2964-6804
DOI: https://doi.org/10.55927/fjst.v4i1.13260
https://journal.formosapublisher.org/index.php/fjst

INTRODUCTION

The Internet of Things (IoT) is revolutionizing national defense by improving situational awareness and real-time data access through sensors and connected devices (IoBT). For example, cloud-based systems can combine camera and sensor data for border monitoring, while RFID devices can track soldiers' health and location

However, IoBT also presents security risks, such as hacking, data theft and malware. In a military context, these threats include illegal remote control, information leakage and signal interference. Therefore, IoBT security requires a holistic approach that considers the operational and information-sharing challenges in a military environment.

Network-based warfare relies on fast information, making IoBT security crucial. Research has exposed IoBT weaknesses in Software-Defined Networking (SDN) as well as the threat of firmware attacks, which are difficult to detect and can give hackers long-term access. The diversity of embedded devices, obsolete components and weak security systems further exacerbate the risks.

Efforts to improve IoBT security include the use of machine learning and a layered approach at the hardware, network and application levels. These findings are important for policymakers in designing robust IoBT security policies.

This research examines best practices for strengthening IoBT security in national defense and their implications for cyber resilience and policy. The focus is on identifying IoBT risks and designing an effective security framework.

THEORETICAL REVIEW

The Internet of Battlefield Things (IoBT) is the future of military operations. By integrating advanced sensor technology, real-time communication, and data processing algorithms, IoBT provides significant tactical advantages on the battlefield. Military forces can gain strategic benefits, including increased situational awareness, faster decision-making, and better unit coordination. IoBT helps monitor border and conflict zone activities, provides health data, assesses risks, and determines critical military personnel locations with precision and speed. However, the implementation of IoBT also involves substantial security risks. Cyberattacks could disrupt military operations, causing data theft, hacking, or physical damage. Therefore, developing a robust security framework to protect against such threats is essential (Sharma, Najjar, & Srinivasan, 2023). With the implementation of IoBT, military operations can be more effective, efficient, and secure.

By definition, the Internet of Battlefield Things (IoBT) is a concept that leverages interconnected devices to increase the effectiveness of military operations, built on the Internet of Things (IoT) paradigm, focused on networking military assets to optimize battlefield efficiency, decision-making, and autonomy (Stocchero et al., 2023).

Network Security and Cybersecurity Strategies in IoBT

In many countries, a comprehensive security framework includes encryption, access control, continuous monitoring, and incident response plans (Espinosa García, Hernández Encinas, & Peinado Domínguez, 2021). Some countries have established Joint Artificial Intelligence Centers to facilitate developing and applying IoBT technology (Bruder, Stockinger, Petrat, & Subtil, 2021). IoBT implementation policies formulated by the Ministry of Defense emphasize the importance of ethical considerations in developing and using IoBT (Canca, 2023). These institutions establish guidelines for the responsible use of IoBT, including compliance with legal and ethical principles, transparency, and accountability. Thus, such an IoBT policy is an excellent example of how a strong security framework and ethical considerations can facilitate the responsible integration of IoBT in military operations.

Implementing robust network security and cybersecurity strategies is crucial in the domain of Internet of Battlefield Things (IoBT), where the integrity and confidentiality of data can determine the success of military operations. These systems are designed to detect unauthorized access or abnormal activities in real-time, enabling immediate responses to potential cyber threats. There are studies have demonstrated the effectiveness of hybrid detection systems that combine signature-based and anomaly-based methods to enhance the detection accuracy in IoBT networks (Jaiswal, Arora, Varshney, & Gupta, 2023; Rosero-Montalvo, István, Tözün, & Hernandez, 2023).

Further, the literature explores the application of comprehensive defense-in-depth strategies that involve multiple layers of security across hardware, software, and network protocols to safeguard IoBT infrastructure. This approach addresses security from the initial design phase, integrating strong encryption methods, secure communication protocols, and continual security updates to protect against evolving threats. Shamsan & Faridi (2022) propose and discuss the integration of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in IoBT settings, which contributes to creating a more adaptable and resilient network defense mechanism. These technologies allow for the dynamic reconfiguration of networks, which is critical in maintaining operational continuity and security in highly variable military operational theatres.

Application of IoBT in Military Logistics and Supply Chain Management

Integrating IoBT technologies into military logistics and supply chain management has significantly enhanced operational efficiencies and resource management. According to recent studies, IoBT facilitates real-time tracking of assets, optimized resource allocation, and improved situational awareness through interconnected sensors and automated systems. For instance, research by Feng, Li, Zeng, & Liu (2020) highlighted how IoBT enables the military to monitor supply routes, assess inventory levels remotely, and predict logistical challenges before they become critical. This proactive approach not only ensures

the timely availability of necessary resources but also minimizes waste and reduces the vulnerability of supply chains to disruption under hostile conditions.

Sensors and communication devices are the linchpins of IoBT, providing the critical data needed for informed decision-making in military operations. These technologies enhance the IoBT's capability to perform real-time surveillance, threat detection, and risk assessment, which is crucial during combat and strategic operations. When a person comes close to a dangerous area like an electric field, riverside, or explosive material, the system will detect the person. It will sound an alarm to inform the authorities. Also, Senel, Kefferpütz, Doycheva, & Elger (2023) show how sensor-fused IoBT systems offer a multi-layered observational network that can detect minute disturbances at or near strategic locations, thereby enabling rapid response and strategic advantage. Moreover, the integration of advanced communication devices ensures that data collected by sensors is relayed back to command centers without delay, allowing for instantaneous strategic decisions that can adapt to changing battlefield conditions and enhance the overall effectiveness of military engagements.

Challenges in Implementing IoBT

Deploying the Internet of Battlefield Things (IoBT) introduces complex challenges concerning security vulnerabilities and system reliability. The literature extensively discusses these challenges, noting that IoBT systems are often targets for cyberattacks due to their critical role in defense operations. Vulnerabilities can stem from various sources, including software bugs, insecure data transmission, and potential physical device tampering. Goel, Somya, Sutar, & Mekala (2023) point out that the heterogeneity of devices and protocols in IoBT systems increases the attack surface, making it challenging to secure every endpoint. Additionally, the real-time requirement of military operations demands exceedingly high reliability and resilience from IoBT systems, challenging engineers to develop solutions operating under extreme conditions without failure.

Significant technological innovations have been proposed and integrated to counter the challenges inherent in IoBT. Artificial Intelligence (AI) and Machine Learning (ML) are at the forefront, offering advanced anomaly detection and predictive maintenance capabilities crucial for preempting failures and cyberattacks. Hussain et al. (2023) illustrate how ML/DL algorithms can analyze vast amounts of data generated by IoBT devices to identify patterns indicative of cyber threats or system malfunctions before they affect operations. Furthermore, Blockchain technology is recognized for its potential to enhance the security of IoBT networks. Blockchain can provide a decentralized and tamper-resistant framework for data integrity, ensuring that unauthorized parties cannot alter or delete communications and operations data (Rashid & Khan, 2022). This application secures data and aids in the traceability of all actions taken within the IoBT.

Synthesis of Literature Review

The literature review emphasizes the vital roles of AI, ML, and Blockchain in addressing significant challenges such as cybersecurity and system reliability on the Internet of Battlefield Things (IoBT). The findings in Section 4 validate these points, demonstrating enhanced threat detection and system responsiveness with AI and ML, alongside stronger security, and data integrity through Blockchain application. These technologies are crucial for securing communications and ensuring the traceability and irrefutability of military operations.

Furthermore, the review identifies several challenges linked to the complex integration and substantial resource requirements of sophisticated IoBT systems, suggesting the necessity for ongoing innovation and customized solutions. To address these challenges effectively, the literature suggests several strategic steps to enhance IoBT security in national defense (Gang, Yu, Huang, & Wang, 2020), including:

a. Conducting rigorous security testing and verification of IoT devices to ensure their resilience against potential cyber threats (Færøy, Yamin, Shukla, & Katt, 2023).
b. Implementing cybersecurity best practices such as strong access controls, data encryption, and network monitoring to safeguard sensitive military data (Munson, 2022).
c. Increasing security awareness and training among military personnel to enhance their readiness in handling IoBT-related security issues (Koller, 2022).

Developing higher education curricula that focus on the use and security aspects of IoBT to prepare future military and technical leaders (Arina, 2021).

METHODOLOGY

We took the first stage by conducting a random study of literature published in the last five years related to our research questions. We then applied a systematic literature review framework based on this literature study. Later, we use a Systematic Literature Review Approach with the following steps (Casasempere-Satorres & Vercher-Ferrándiz, 2020; Kuckartz & Rädiker, 2019):

a. Article Selection: This was conducted based on bibliometrics. Zotero bibliometrics was imported into the SLR tool MaxQDA, and the title, abstract, and keywords were read to ensure relevance to the research topic.
b. Import PDF Files: Each article is attached to the SLR tool for easy management and reference.
c. Data Extraction: This is done by coding to collect information about IoBT security best practices, potential study topics, and research recommendations, as well as categorizing data based on themes or sub-themes.

d. Data Analysis: Involves synthesizing and interpreting collected data, as well as identifying patterns and trends in best practices, study topics, and research recommendations.
e. Reporting Results: Findings from the SLR are presented systematically, and the implications of the findings for research and practice are discussed.

The inclusion criteria applied include:

a. Thematic Relevance & IoBT Security Taxonomy: Resources that explicitly discuss IoBT security, its application in national protection, or best cybersecurity practices that can apply to IoBT.
b. Research Quality: Studies conducted with solid methodology, including empirical research, systematic reviews, or case analysis.

Exclusion Criteria include:

a. Geographical Limitations: Studies focusing only on a specific geographic context are irrelevant to the global scope or national maintenance application.
b. Not Focused on Security: Resources that discuss IoBT from a non-security perspective unless they provide direct insight into security issues.
c. Unavailability: Articles must be completed or contain essential information such as titles, abstracts, keywords, contents, and references.

The comprehensive IoBT vulnerability taxonomy will provide a robust framework for identifying various vulnerable aspects of the IoBT system, especially in the context of state protection. The current vulnerabilities taxonomy in the context of the Internet of Battlefield Things still needs to be explored. To meet the objectives of this study, we summarized several taxonomies (Abbas, Hashmat, & Shah, 2020; Azzedin & Alhejri, 2022; Bhardwaj, Kaushik, & Kumar, 2022; Bou-Harb & Neshenko, 2020; Garg, Singh, Sharma, & Sharma, 2022; Hemmati & Rahmani, 2022) that focus on improving security in IoT systems, including IoBT, on ensuring robust protection against potential attacks. The taxonomy summary looks at essential elements ranging from hardware to policy. This taxonomy summary provides an in-depth understanding of the various vulnerabilities' governments must consider in developing security strategies. The following is an outline of the IoBT vulnerability taxonomy structure as a basis for the work of this study:

a. Hardware: It is important to ensure the security of sensors, actuators, and communication components to protect data integrity and IoBT system operations.
b. Software: The operating system, firmware, and applications/services focus on maintaining device security. It emphasizes securing IoT devices' code, configuration, and application processes.
c. Network and Communications: This aspect highlights the importance of the security of communications protocols and network infrastructure to

prevent eavesdropping, data manipulation, or interference with transmissions.

d. Data and Information: Data integrity and confidentiality are the focus in protecting sensitive information or military secrets from unauthorized access or manipulation.
e. Human and System Interaction: Involving the user interface and training as a focal point ensures that human interaction with the IoBT system does not open opportunities for attacks or unintentional human error.
f. Policies and Procedures: Strong security policies and effective risk management are important in addressing threats that may arise using IoBT systems.
g. Operational Environment: Physical aspects and physical threats are important to consider in the operational environment where the IoBT system will be used, including physical conditions and potential physical threats.

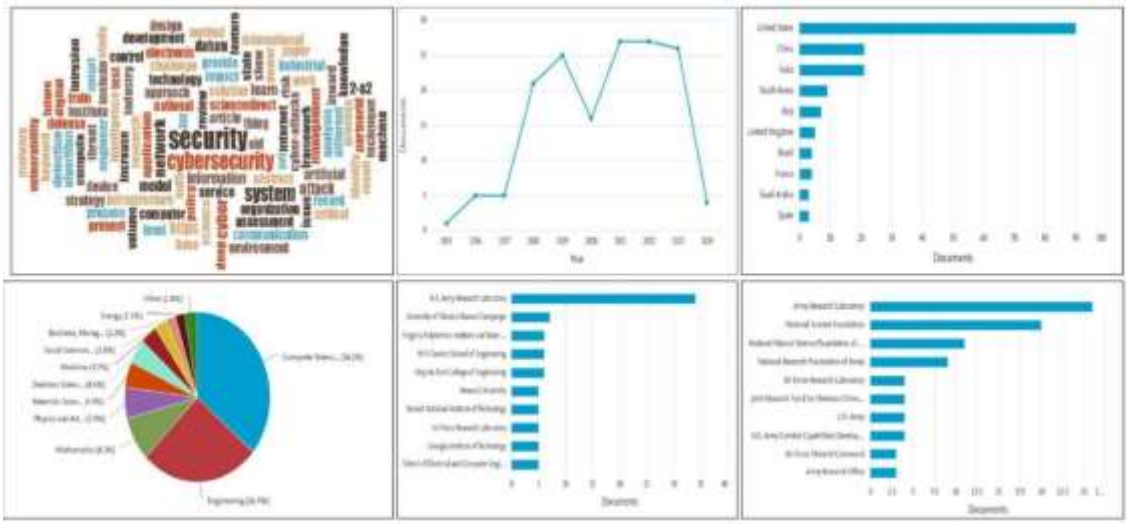
This taxonomy summary provides a solid foundation for identifying, analyzing, and addressing threats in IoBT systems, enabling the development of effective security strategies to protect assets and ensure smooth operations in the context of homeland protection.

RESULTS AND DISCUSSION

IoBT Document Data Description

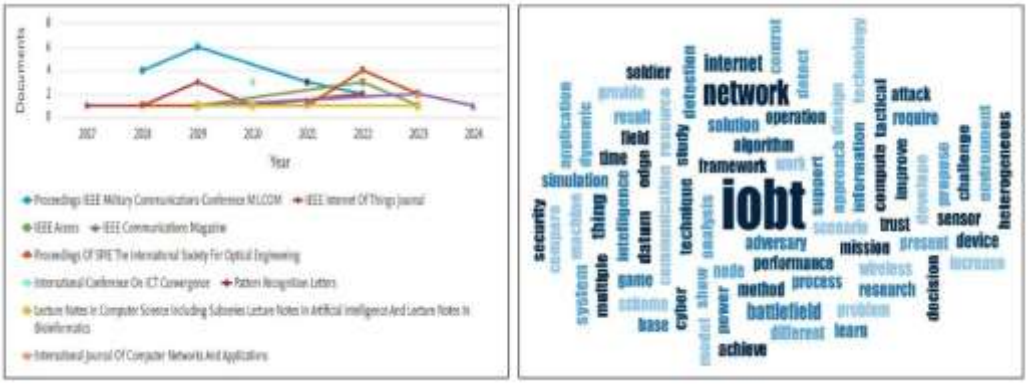
The data description provided involves collecting articles about the Internet of Things (IoT) and the Internet of Battlefield Things (IoBT) by applying relevant search keywords. This data was obtained from the ScienceDirect and Scopus repositories with a publication period between 2015 and 2024. After applying the inclusion and exclusion process, 3471 relevant article titles were analyzed further. From this analysis, 157 article titles were obtained based on the research objectives. In addition, of the 157 titles, only 122 articles were complete and relevant to IoBT, while the other 35 articles were not available in paper form.

Data visualization was conducted by visualizing the abstracts of article titles related to IoBT, which included word-cloud visualization of the titles, abstracts, and keywords of 122 articles. It aims to provide a clearer and easier-to-understand picture of the focus and research topics covered in the literature that has been collected.



Source:

Figure 1. Wordcloud has 3,471 article titles, IoBT publication trends, IoBT by Author Country, Subject area, Research affiliation, and Sponsor.

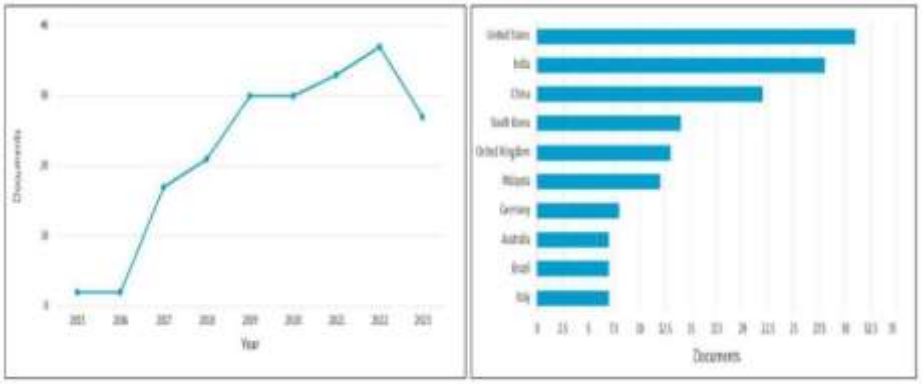


Source:

Figure 2. IoBT document publication sources and Wordcloud of 122 IoBT journal articles.

IoT Policy Document

The IoT policy documents obtained from the screening results were 199 titles (2%) from 10,143 search result titles originating from 2419 Scopus repository articles and 7724 ScienceDirect repository articles. In the 199 titles of this article, IoT and IoBT are either mentioned or both are mentioned. Figures 9 and 10 are descriptions of the data.



Source:

Figure 3. Journal publication trends and IoT Policy articles by Author Country (199 titles) 2015-23

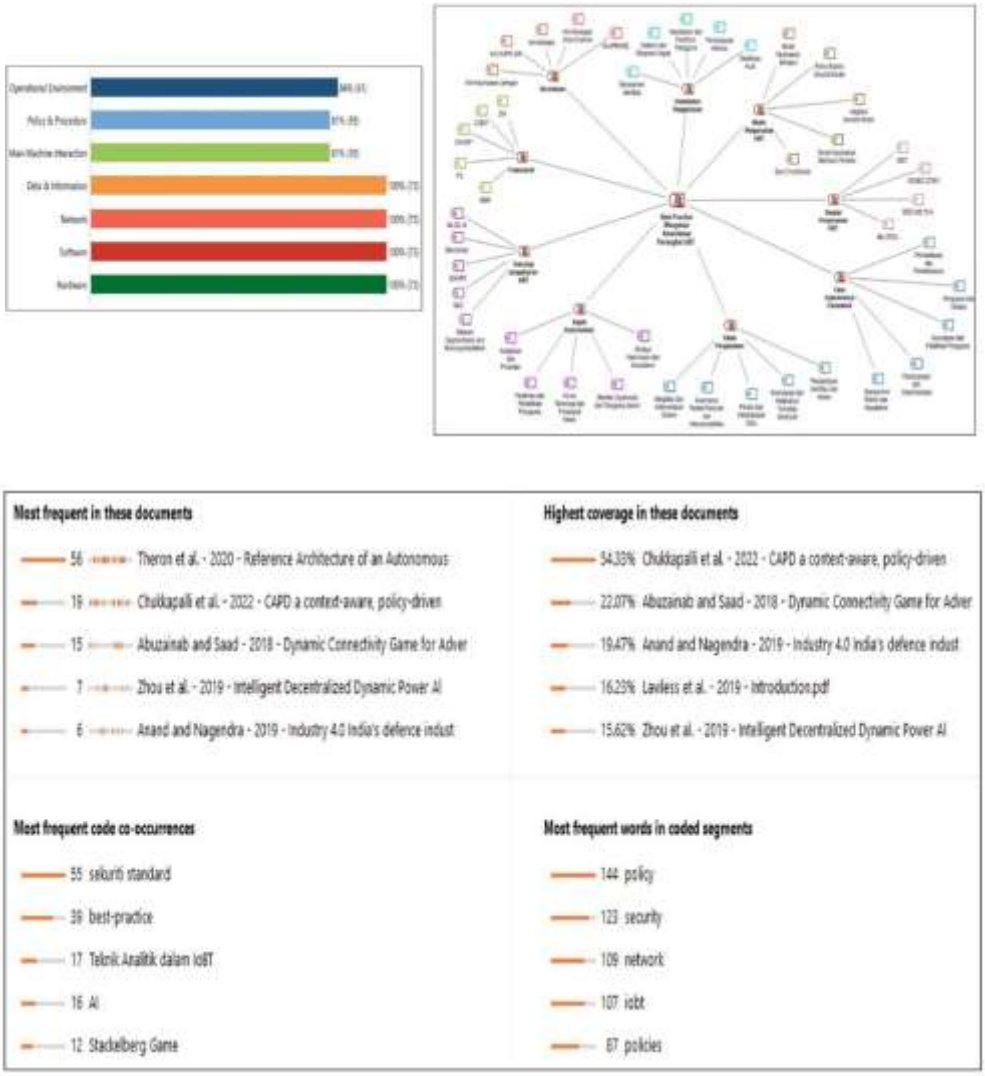
Furthermore, by looking at the availability of complete papers and their suitability to the IoBT search results, only 122 article titles were used in this study as the basis for this general analysis of the SLR.

IoBT Vulnerability Taxonomy

In this study, a reflection of the IoBT vulnerability taxonomy, which is classified based on the main system aspects that are vulnerable to attack or failure, can be identified in Figure 4 below. From the data identified based on taxonomy, there were 73 relevant articles from a total of 122 titles. All taxonomy categories, namely Data & Information and Network, cover percentages above 80% to 100%. It shows that these articles are truly relevant to the taxonomic categories that have been determined. Furthermore, these 73 articles formed the basis of the primary analysis in this study.

One of the topics discussed in the study is how to improve IoT device security. To achieve these goals, multi-layer defense-in-depth cybersecurity mechanisms can be implemented at the hardware, network, and application levels. This mechanism aims to ensure the timely and secure dissemination of information obtained from interconnected devices, such as radars, uncrewed aerial vehicles (UAVs), sensors, armored fighting vehicles, and wearable devices. Software-defined networking (SDN) can also help manage network services and increase resilience against cyber-attacks. Additionally, to strengthen the cybersecurity aspect of IoBT, a multi-faceted intrusion detection system that combines ensemble methods with supervised machine learning can be used to detect and report anomalies. This approach helps maintain the integrity and confidentiality of shared data, preventing tampering, errors, and hacking.

Figure 4 shows how the SLR study was coded to generate answers to this research question. The coding process using the taxonomy structure and its derived sub-codes resulted in 5979 document segments, which were then analyzed individually.



Source:

Figure 4. Thematic analysis frame of reference best practices for overcoming IoT/IoBT System vulnerabilities, and Matrix of exploration results of 122 IoBT articles divided into 5979 document segments.

IoT Best Practices and Security Framework

Main Vulnerabilities of IoT Devices

The principal vulnerabilities of Internet of Things (IoT) devices include security, privacy, interoperability, and standard licensing. IoT devices are vulnerable to hostile operations, financial gain, and access to sensitive data due to persistent online connectivity and weakening security measures. Common vulnerabilities found in IoT devices include outdated components, propagating NAT-PMP information, remote telnet access, Heartbleed vulnerability, Ticketbleed vulnerability, expired SSL certificates, insecure default settings, default SNMP agent community name, running on non-standard ports, and a generic or default password. Additionally, IoT devices are susceptible to vulnerabilities in the external path arising from interactions between physical and digital systems that can have serious consequences. Cryptography misuse is another vulnerability that compromises the privacy of sensitive data in IoT

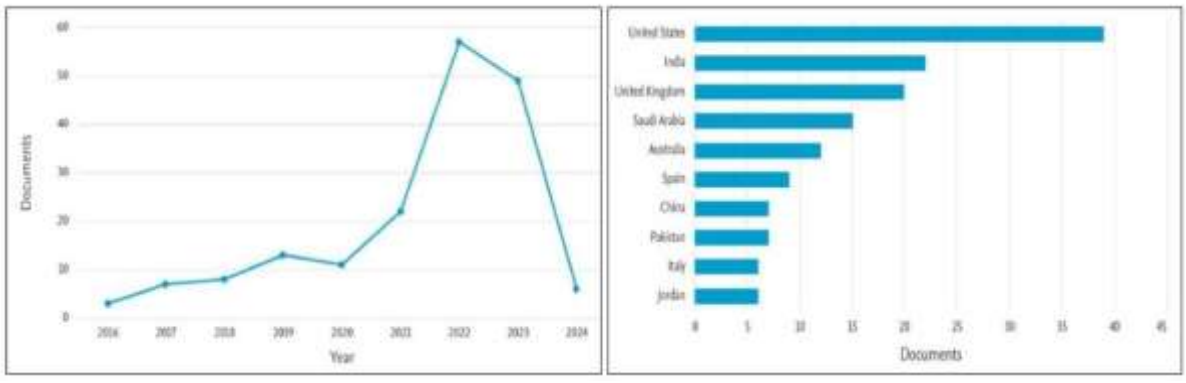
devices. In general, the number of articles discussing IoT device vulnerability issues was 24 articles (19.7%). However, more articles discussed violations of security standards, namely 59 articles (48.4%).

Stackelberg Game Scheme for IoBT Security

Network connectivity issues are studied for adversarial Internet of Battlefield Things (IoBT) systems where attackers aim to disrupt network connectivity by trying to compromise one of the IoBT nodes at a time (antagonistic). To counter such attacks, IoBT defenders attempt to reestablish IoBT connectivity by deploying new IoBT nodes or changing existing nodes' roles. These problems are formulated as dynamic multistage Stackelberg connectivity games that extend classical connectivity games and explicitly consider the characteristics and requirements of IoBT networks. Specifically, defender imbalances include IoBT latency and the weighted number of disconnected nodes at each stage of the game. Due to the actions of attackers and defenders at each stage of the game on the network state, we use the Stackelberg balance (FSE) feedback solution to solve the IoBT connectivity game. Then, the sufficient conditions under which the IoT system will remain connected are determined by the FSE solution analytically. Numerical results show that the expected number of disconnected sensors when the FSE solution is applied is reduced by up to 46% compared to the basic scenario of a Stackelberg game without feedback and by up to 43% compared to the same basic probability policy. In this SLR, 12 articles (9.8%) discuss the Stackelberg game scheme for IoT security.

Best Practices for IoT Security in the Field of National Defense

Figure 14 shows a line graph of IoT Security best-practice articles from 2015 to 2024. The number of IoT Security best-practice articles has increased rapidly from 2015 to 2024. Although there were slight restrictions from year to year, significant strengthening occurred in 2017, 2020, and 2023.



Source:

Figure 5. IoT Security best practices trend articles, and IoT Security best practices articles by country

This trend shows increased awareness of the importance of IoT security and the need for best practices. It is driven by several factors, such as the

increasing number and complexity of cyberattacks on IoT devices and regulations that require the implementation of IoT security, such as the General Data Protection Regulation in the European Union (Hoofnagle et al., 2018) and, Increasing IoT adoption in various sectors, such as industry, health, transportation, national defense (IoBT).

Several factors can cause fluctuations from year to year, for example Security Events such as WannaCry and Mirai in the period 2017 and 2020 – the peak popularity of the WannaCry attack was May 12 2017, infecting more than 230,000 computers in 150 countries - Mirai peaked with 600 thousand infections during late 2016 (Manos Antonakakis, 2017) highlighted the need to improve cyber security and implement strategies to respond quickly to future attacks; while the spike in 2023 was caused by publications due to the need for new best-practice guidelines or revisions to old guidelines (Barrera et al., 2023; Bellman, 2022).

This trend also shows that the IoT industry is increasingly focusing on security. It is positive because security is essential to developing and implementing IoT, including IoBT. The increasing number of articles shows a wealth of information and resources available for organizations looking to improve their IoT security. However, several challenges still need to be overcome, such as technological complexity, lack of skills, and market fragmentation.

While challenges remain, these trends show that the IoT industry is moving in the right direction regarding security. By continuing to increase awareness and best practices, IoT security can be improved, and the risk of cyberattacks can be reduced. Figure 15 shows the authors' countries of origin regarding IoT Security best practice insights and proposals.

This SLR study has identified various IoBT security best practices that can be applied to improve the security of IoBT systems in national defense. The three main clusters of collaborative best practices include the development of robust security standards, implementing effective security measures, and Increasing awareness and training. This cluster description includes seven developments of robust security standards for IoT devices covering hardware, software, and communications security requirements.

1) Implementation of strict security testing and verification of IoBT devices before use.
2) Implement cybersecurity practices such as strong access controls, data encryption, and network monitoring.
3) Public and Private Sector Collaboration through the creation and activities of communities/alliances/forums.
4) Cybersecurity Training and Simulation.
5) Increased security awareness and training for military personnel regarding risks and how to use IoT devices safely.
6) The development of a higher education curriculum is related to aspects of IoBT use and security.

7) IoT Collaborative Best Practices are critical to building a secure and trusted ecosystem. By working together, parties can help protect user data and privacy and drive responsible IoT-IoBT growth and adoption.

Topic for Studying the Security Potential of IoT in the Field of National Defense

In this analysis, 48 articles (39%) specifically suggested improving IoBT security as a critical topic in implementing device integration into the IoBT context. Meanwhile, the topic of analytical techniques also featured a lot of discussion highlights, namely 47 articles (38.5%). In Figure 16, of the 122 article files reviewed in the SLR study, 73 files are described for the IoBT system security study topic. Six uncoded titles (not included in the search category using a coding system), so only 67 articles were analyzed and classified based on their study topic coding. It shows that only a tiny proportion of the articles described are theoretical or conceptual.

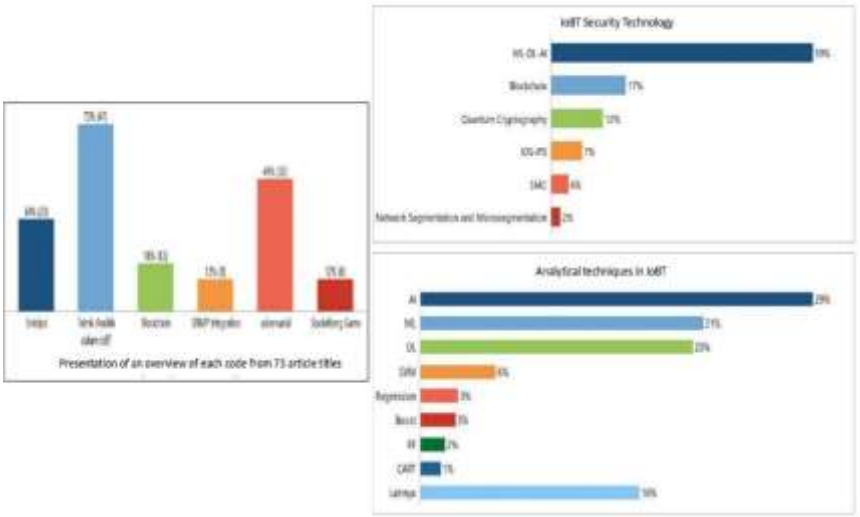
Internet of Things (IoT) security potential study topics analyze the performance of security mechanisms on IoT development platforms, such as the Raspberry Pi. Another topic is understanding the relationship between security threats, standards, implementation, and network security in real-world IoT applications. Additionally, other research focuses on securing IoT devices and networks and protecting personal safety while ensuring accessibility. In this latter regard, there is a need to address resource constraints and vulnerabilities in IoT infrastructure to reduce opportunities for cyber-attacks, such as overcoming low computing power and limited storage (Krichen, 2023; Mei et al., 2023). For example, context reveals and exposes the operation of dark-net traffic detection systems in IoT networks and discusses areas such as privacy provisioning, lightweight cryptographic frameworks, secure routing, resilience, and DoS/DDoS attacks. Context of the need for increased security integration in resource constrained IoT devices and recommendation of a lightweight deep learning approach for monitoring malware in real-time.

Additionally, the context discusses the effectiveness of artificial intelligence (AI), deep learning (DL), and machine learning (ML) techniques for IoT security, highlighting the role of AI in enhancing traditional cybersecurity. Topics of interest also include privacy provisioning, lightweight cryptographic frameworks, secure routing, resilience, defense against DoS or DDoS attacks in IoT networks, and analytical techniques practical in the detection, including artificial intelligence. Overall, these topics contribute to improving IoT systems' security and addressing their unique challenges.

In the context of the specific implementation of security for the Internet of Battlefield Things (IoBT), the expansion and deepening of the topic includes an in-depth analysis of the vulnerabilities of IoBT sensors, especially against cyber-attacks, and detection strategies that utilize the latest technologies such as machine learning (ML), deep learning (DL), and artificial intelligence (AI) to improve accuracy. An emphasis on security coordination through innovative approaches, such as stochastic geometry and heuristic algorithms, offers a solution to improve constructive collaboration in IoBT networks. The importance of reputation-based trust models for identifying and isolating malicious elements

from networks highlights adaptive strategies in dealing with threats. On the other hand, exploration of the challenges of scale, heterogeneity, and network dynamics, as well as internal threats, supports the development of more resilient and dynamic IoT systems. This discussion should be enriched with case studies and empirical data to demonstrate the practical application of the presented security theory and analyze the effectiveness of various analytical techniques in absolute protection contexts. This integration approach is expected to more effectively address IoBT vulnerabilities, ensuring system confidentiality and security in military operations.

Figure 6 shows that the top two topics are Analytical Techniques, with 47 articles (70.1%), and Adversarial techniques, with 33 articles (49%). It indicates that current IoBT research focuses on developing and applying analytical techniques to improve the security of IoBT systems. Some analytical techniques used in IoBT include log data analysis to detect anomalies and attacks, network analysis to identify vulnerabilities and threats, and Machine Learning and Deep Learning to predict and prevent attacks. Like Analytical Techniques, IoBT system security study topics related to Adversarial attacks and defenses are one of the main challenges in IoBT system security research. Research on this topic focuses on understanding and modeling adversarial behavior and developing techniques to detect and prevent adversarial attacks.



Source:

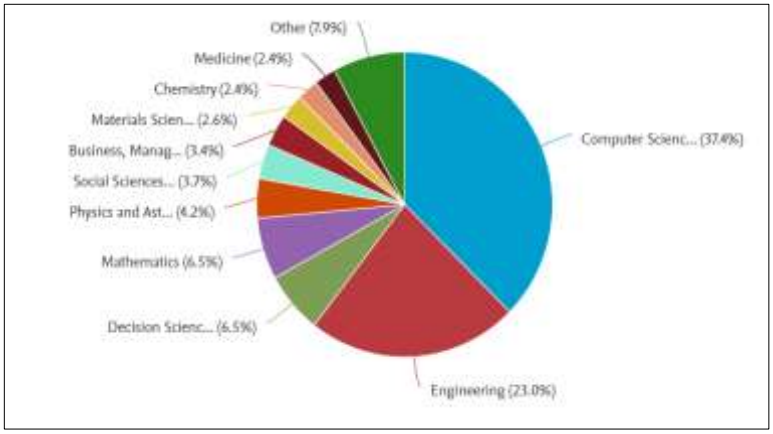
Figure 6. Percentage of discussions on IoBT system security study topics, number of articles about system security technology, and IoBT analytical techniques

Meanwhile, next in line is Encryption, which has 23 articles (34%). Encryption is a technique currently developing, namely the process of converting data into cipher text using algorithms and encryption keys to protect the confidentiality of information, so it has the potential to increase the security of the IoBT system. Meanwhile, with 12 articles (18%), Blockchain is a potential application in IoBT architecture, such as identity and access management, secure data storage, and device tracking and auditing. *Blockchain* is a technology used to store transaction records decentralized and securely. Blockchain uses connected and encrypted data structures to create an immutable chain of blocks.

Studies on securing IoBT with SNMP Integration and Stackelberg Game identified eight articles each (12%). SNMP is a protocol that is widely used to manage network devices. SNMP integration with IoBT systems can improve security by debugging devices for vulnerabilities, applying security patches, and detecting and responding to attacks. Stackelberg game is a theory model that can analyze interactions between defenders and attackers in IoBT systems. Research on this topic focuses on developing optimal strategies for Defender and understanding the impact of numerous factors on the security of IoBT systems.

The high interest in AI, DL, and ML reflects the current trend in IoBT research, where these techniques are considered to have exciting potential in addressing complex and dynamic challenges on the battlefield. AI, with its ability to process and analyze big data in real-time; DL, with its power to recognize patterns from unstructured data; and ML, with its adaptability in learning and improving performance based on new data, all make essential contributions to developing effective IoT solutions.

In the context of IoBT research/studies, where speed, accuracy, and adaptability are critical, applying AI, DL, and ML offers promising solutions. This analysis shows that the research community recognizes this potential and actively explores techniques to improve IoBT capabilities. With AI, DL, and ML, IoT systems can better interpret data from multiple sensors and sources in real-time, enabling faster and more informed decisions on the battlefield. In conclusion, these SLR results demonstrate a strong focus on AI, DL, and ML in IoBT research, reflecting current trends and the exciting potential of these techniques in overcoming IoBT challenges, for example, for the sensor case study by Xiaowei (2023) by SLR inferences This. It is hoped that further research will continue to develop and optimize the application of these techniques in IoBT, paving the way for innovation and technological advances that can significantly increase the effectiveness and efficiency of military operations. Also, this SLR study provides valuable insights into the current and future directions of IoBT research, highlighting the importance of AI, DL, and ML in developing more sophisticated and adaptive solutions to IoBT implementation challenges in national defense.



Source:

Figure 7. IoBT Security best practice subject areas

a. Figure 7 shows the percentage of best-practice subject areas (not the number). Of the 122 articles identified, two IoT security best-practice subject areas were most discussed, namely Computer Science with a percentage of 37.4% and Engineering with 23%. These two subjects are the primary basis for implementing IoT and IoBT security.
b. Decision science and Mathematics, with 6.5% each, are two sciences that are considered necessary in studying IoBT system security. Furthermore, physics, social science, business, material science, chemistry, and medicine are the following reviews that will also receive attention in studying IoBT system security. It shows the importance of securing IoT systems, devices, and firmware from vulnerabilities and malware.
c. Meanwhile, Figure 20 shows the types of IoBT devices reviewed in this study. In this IoBT system, there are various types of devices identified in this SLR to show researchers' attention to IoBT system devices, including:
d. a. Sensors and Actuators (97%). In this study, most of the research reviews sensors and actuators, which shows the main research trends in the last ten years. Sensors detect environmental conditions or enemy activity, and actuators perform actions based on sensor data, such as automated surveillance or defense systems.
e. Communication Devices (59%). Communication devices that enable real-time exchange of data and information between units on the battlefield have received the attention of researchers in the last ten years.
f. Unmanned Air Vehicles - UAVs (51%). UAVs, also known as drones, are unmanned aircraft that can be operated remotely or fly automatically via a programmed flight control system. UAVs are used in various military applications, including reconnaissance, surveillance, intelligence gathering, and attacks. Some examples of UAVs that are often used in military operations are the MQ-9 Reaper, RQ-4 Global Hawk, Predator, Bayraktar TB2 (tactical UAV developed by Turkey), DJI Phantom, and X-47B (experimental UAV designed for take-off operations and landings from aircraft carriers, demonstrating the capabilities of UAVs in naval operations). These UAVs offer diverse capabilities, from long-range reconnaissance to precision strikes, and have become integral to modern military operations.
g. Wearables & Camera Devices (41%). Wearable devices by military personnel, such as smartwatches or augmented reality glasses, improve situational awareness and communications.
h. Unmanned Ground Vehicles – UGVs (39%) are ground combat vehicles operated automatically or remotely for various missions, such as surveillance or logistics transport.
i. Unmanned Maritime Vehicles – UMVs (10%) are unmanned maritime combat vehicles used for reconnaissance, minesweeping, or oceanographic data collection operations.
j. Command and Control Systems (10%) integrate information from various sources to support decision making and coordination of military operations.

It can be briefly seen in Figure 7 that AI technology, Blockchain, intrusion detection and prevention have dominated article reviews in the last ten years. Quantum cryptography is a technology that is starting to emerge and will likely revolutionize cybersecurity technology shortly. Quantum cryptography has the potential to provide secure communication channels and build unbreakable encryption systems. Quantum key distribution (QKD) is a promising scheme for secure communications, as it exploits the principles of quantum mechanics to distribute cryptographic keys over public channels. Researchers are progressing toward achieving secure and reliable quantum communication systems by overcoming practical imperfections and vulnerabilities, such as modulation leaks and dependence on quantum memory (Renner & Wolf, 2023).

CONCLUSION NAD RECOMMENDATION

There are three main clusters of collaboration: Developing solid security standards, implementing adequate security measures, and Increasing awareness and training. The third collaborative cluster is described in seven steps for implementing IoT device security such as:

a. Development of Security Standards and Integration with International Security Standards: Develop robust security standards for IoBT devices, covering hardware, software, and communications security requirements; and integrate security standards developed with international standards such as ISO/IEC 27001 for information security management and NIST for cybersecurity frameworks. This integration ensures that IoBT security meets national needs and aligns with global best practices.
b. Security Testing and Verification: Conduct rigorous security testing and verification of IoBT devices before use. Cybersecurity Practices attention testing: Implementing cybersecurity practices, including robust access control, data encryption, and network monitoring using Blockchain Technology, Machine Learning for Threat Detection, and Zero Trust Architecture.
c. Identity and Access Management: Strengthen identity and access management (IAM) with multi-factor authentication (MFA) technologies and public/private key management to control access to IoBT devices and data. It is essential to prevent unauthorized access and ensure that only functioning users or devices can access sensitive information. Supporting things are needed, such as public and private sector collaboration, cyber security training and simulation, increased security awareness and training, and IoBT-specific cyber threat assessment, a study of the specific cyber threats facing IoBT, and how to overcome these challenges.

FURTHER STUDY

Future research is expected to further explore this material.

REFERENCES

Abbas, S. G., Hashmat, F., & Shah, G. A. (2020). A Multi-layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1820–1825. Guangzhou, China: IEEE. doi: 10.1109/TrustCom50675.2020.00249

Abel, E., Muhammad Shafie, A. L., & Howe Chan, W. (2021). Deployment of internet of things-based cloudlet-cloud for surveillance operations. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *10*(1), 24. doi: 10.11591/ijai.v10.i1.pp24-34

Agarwal, S., Agarwal, V. D., Mittal, V., & Agarwal, I. (2023). Review of Effect of Internet of Things(IoT) in Cybercrime. *International Journal for Research in Applied Science and Engineering Technology*, *11*(6), 4672–4678. doi: 10.22214/ijraset.2023.54519

Arina, A. (2021). Analysis of IoT security issues used in Higher Education Institutions. *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH*, *09*(05). doi: 10.47191/ijmcr/v9i5.01

Azzedin, F., & Alhejri, I. (2022). A Layered Taxonomy of Internet of Things Attacks. *Proceedings of the 6th International Conference on Future Networks & Distributed Systems*, 631–636. Tashkent TAS Uzbekistan: ACM. doi: 10.1145/3584202.3584297

Bhardwaj, A., Kaushik, K., & Kumar, M. (2022). Taxonomy of Security Attacks on Internet of Things. In O. Kaiwartya, K. Kaushik, S. K. Gupta, A. Mishra, & M. Kumar (Eds.), *Security and Privacy in Cyberspace* (pp. 1–24). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-19-1960-2_1

Bou-Harb, E., & Neshenko, N. (2020). Taxonomy of IoT Vulnerabilities. In E. Bou-Harb & N. Neshenko, *Cyber Threat Intelligence for the Internet of Things* (pp. 7–58). Cham: Springer International Publishing. doi: 10.1007/978-3-030-45858-4_2

Bruder, R., Stockinger, C., Petrat, D., & Subtil, I. (2021). Development of Cooperative Artificial Intelligence (AI) Applications to Support Human Work in Manufacturing. In N. L. Black, W. P. Neumann, & I. Noy (Eds.), *Proceedings of the 21st Congress of the International Ergonomics Association (IEA 2021)* (pp. 391–397). Cham: Springer International Publishing. doi: 10.1007/978-3-030-74608-7_49

Canca, C. (2023). AI Ethics and Governance in Defence Innovation. In M. Raska & R. A. Bitzinger, *The AI Wave in Defence Innovation* (1st ed., pp. 59–79). London: Routledge. doi: 10.4324/9781003218326-4

Casasempere-Satorres, A., & Vercher-Ferrándiz, M. L. (2020). Análisis Documental Bibliográfico. Obteniendo El Máximo Rendimiento A La Revisión De La Literatura En Investigaciones Cualitativas. In F. Freitas, I. Pinho, A. I. Rodrigues, B. M. Faria, & A. Pedro, *New Trends In Qualitative Research* (pp. 247–257). Ludomedia. doi: 10.36367/ntqr.4.2020.247-257

Dwaraka Srihith I., David Donald A., Aditya Sai Srinivas T., Anjali D., & Chandana A. (2023). Firmware Attacks: The Silent Threat to Your IoT

Connected Devices. *International Journal of Advanced Research in Science, Communication and Technology*, 145–154. doi: 10.48175/IJARSCT-9104

Espinosa García, J., Hernández Encinas, L., & Peinado Domínguez, A. (2021). A Comprehensive Security Framework Proposal to Contribute to Sustainability. *Sustainability*, *13*(12), 6901. doi: 10.3390/su13126901

Færøy, F., Yamin, M., Shukla, A., & Katt, B. (2023). Automatic Verification and Execution of Cyber Attack on IoT Devices. *Sensors*, *23*(2), 733. doi: 10.3390/s23020733

Feng, Y., Li, M., Zeng, C., & Liu, H. (2020). Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. *Entropy*, *22*(10), 1166. (F:JURNALIOBT). doi: 10.3390/e22101166

Gang, Z.-H., Yu, C.-Y., Huang, H.-B., & Wang, L.-J. (2020). Research on International and Domestic Internet of Things Security Policy. *2020 2nd International Conference on Information Technology and Computer Application (ITCA)*, 521–524. Guangzhou, China: IEEE. doi: 10.1109/ITCA52113.2020.00115

Garg, A., Singh, A., Sharma, K., & Sharma, V. (2022). A Taxonomy for Internet of Things in Security Distributed Denial of Service Attacks. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 1274–1281. Greater Noida, India: IEEE. doi: 10.1109/ICAC3N56670.2022.10074432

Goel, S., Somya, Sutar, S., & Mekala, P. (2023). Malicious Node Detection in Heterogeneous Internet of Things. In A. K. Dubey, V. Sugumaran, & P. H. J. Chong (Eds.), *Advanced IoT Sensors, Networks and Systems* (pp. 155–172). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-99-1312-1_13

Haas, Z. J., Culver, T. L., & Sarac, K. (2021). Vulnerability Challenges of Software Defined Networking. *IEEE Communications Magazine*, *59*(7), 88–93. doi: 10.1109/MCOM.001.2100128

Hemmati, A., & Rahmani, A. M. (2022). The Internet of Autonomous Things applications: A taxonomy, technologies, and future directions. *Internet of Things*, *20*, 100635. doi: 10.1016/j.iot.2022.100635

Hussain, A., Sharif, H., Rehman, F., Kirn, H., Sadiq, A., Khan, M. S., … Chandio, A. H. (2023). A Systematic Review of Intrusion Detection Systems in Internet of Things Using ML and DL. *2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 1–5. Sukkur, Pakistan: IEEE. doi: 10.1109/iCoMET57998.2023.10099142

Jaiswal, D., Arora, K., Varshney, M., & Gupta, T. (2023). A Hybrid Method for Network Intrusion Detection. *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 732–738. Jalandhar, India: IEEE. doi: 10.1109/ICSCCC58608.2023.10176754

Kanciak, K., Jarosz, M., Glebocki, P., & Wrona, K. (2021). Enabling civil-military information sharing in federated smart environments. *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 897–902. New Orleans, LA, USA: IEEE. doi: 10.1109/WF-IoT51360.2021.9595715

Koller, M. (2022). Recommendations for Safety-Conscious Smart Device Use by Military Professionals. *Academic and Applied Research in Military and Public Management Science*, *21*(2), 5–14. doi: 10.32565/aarms.2022.2.1

Li, M., Yu, Y., & Zou, Y. (2023). IoT devices firmware security detection based on static analysis technology. In L. Wang & X. Liu (Eds.), *International Conference on Intelligent Systems, Communications, and Computer Networks (ISCCN 2023)* (p. 82). Changsha, China: SPIE. doi: 10.1117/12.2679937

Mera, A. (2022). *Holistic methods for protecting and testing embedded devices* (Northeastern University). Northeastern University. doi: 10.17760/D20467199

Munson, K. A. H. (2022). Considerations for a Successful Cybersecurity Program. In V. A. Suveiu, *Routledge Handbook of Risk Management and the Law* (1st ed., pp. 265–279). New York: Routledge. doi: 10.4324/9781351107242-24

Rajasekar, V. R., & Rajkumar, S. (2023). A Study on Internet of Things Devices Vulnerabilities using Shodan. *International Journal of Computing*, 149–158. doi: 10.47839/ijc.22.2.3084

Rashid, A., & Khan, A. U. R. (2022). Blockchain-Based Autonomous Authentication and Integrity for Internet of Battlefield Things in C3I System. *IEEE Access*, *10*, 91572–91587. (F:JURNALIOBT). doi: 10.1109/ACCESS.2022.3201815

Rosero-Montalvo, P. D., István, Z., Tözün, P., & Hernandez, W. (2023). Hybrid Anomaly Detection Model on Trusted IoT Devices. *IEEE Internet of Things Journal*, *10*(12), 10959–10969. doi: 10.1109/JIOT.2023.3243037

Senel, N., Kefferpütz, K., Doycheva, K., & Elger, G. (2023). Multi-Sensor Data Fusion for Real-Time Multi-Object Tracking. *Processes*, *11*(2), 501. doi: 10.3390/pr11020501

Sharma, P., Najjar, L., & Srinivasan, S. (2023). Practical Applications to Prevent Cyberattacks on Internet on Battlefield Things (IoBT). *Advanced Information Technologies and Applications*, 17–24. Academy and Industry Research Collaboration Center (AIRCC). doi: 10.5121/csit.2023.130602

Stocchero, J. M., Silva, C. A., De Souza Silva, L., Lawisch, M. A., Dos Anjos, J. C. S., & De Freitas, E. P. (2023). Secure Command and Control for Internet of Battle Things Using Novel Network Paradigms. *IEEE Communications Magazine*, *61*(5), 166–172. doi: 10.1109/MCOM.001.2101072

Swathi, Dr. N. (2022). Situational awareness and risk assessment during armed conflict using ceaseless video monitoring via IoMT. *International Journal of Scientific Research in Engineering and Management*, *06*(05). doi: 10.55041/IJSREM13459

Tuscano, A., & Joshi, S. (2023). Significance of Cyber Security of IoT devices in the Healthcare Sector. *2023 Somaiya International Conference on Technology and Information Management (SICTIM)*, 12–16. Mumbai, India: IEEE. doi: 10.1109/SICTIM56495.2023.10104657