International Journal of Scientific Engineering and Science
Volume 7, Issue 5, pp. 115-118, 2023. ISSN (Online): 2456-7361

Internet of Things (IoT) in Defense and Security Systems: A Literature Review

Ummiati Rahmah[1], Mahmud Mustapa[1], Putri. I S Samad[1], Nur Azizah Eka Budiarti[2]
[1]Electronic Engineering Education, Makassar State University, Makassar, Indonesia
[2]Computer Science Department, IPB University, Bogor, Indonesia
Corresponding author: Ummiati Rahmah
Email: ummiati.rahmah@unm.ac.id, mahmud.mustapa@unm.ac.id, putri.ida@unm.ac.id, 97_nurazizah@apps.ipb.ac.id

Abstract— *The Internet of Things (IoT) has become a major trend in the field of information and communication technology. In the context of defense and security systems, IoT offers the potential to improve effectiveness, surveillance, and responsiveness in military and security operations. This article aims to present a literature review on the application of IoT in defense and security systems, focusing on technical aspects, advantages, challenges, and future research directions. Through an analysis of various related literature sources, this article identifies key trends, expected benefits, and issues that need to be considered in adopting IoT in defense and security systems.*

Keywords— *Internet of Things (IoT), defense system, security system, literature review, advantages, challeges.*

I. INTRODUCTION

The Internet of Things (IoT) has become a major trend in the field of information and communication technology. This concept refers to a network consisting of physical objects that are interconnected and can exchange data over the Internet [1]. IoT has found wide application in various sectors, including defense and security systems (Figure 1). In this context, IoT offers the potential to improve efficiency, surveillance, and responsiveness in military and security operations [2]

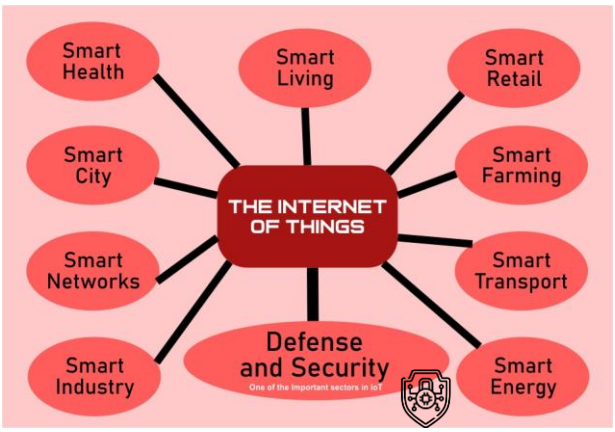

Fig. 1. Various sector IoT

Defense and security systems play a crucial role in maintaining the stability and security of a country or region. The rapid development of technology requires defense and security systems to adapt and use innovative solutions that can improve their capabilities and responsiveness. One of the prominent solutions is the application of IoT in the context of defense and security systems[3].

This article aims to present a literature review on the application of IoT in defense and security systems. This literature review covers the technical aspects, advantages, challenges, and future research directions of adopting IoT in defense and security systems. By analyzing various related literature sources, this article identifies key trends, expected benefits, and issues that need to be considered in integrating IoT into defense and security systems[4].

By gaining comprehensive insights through the literature review, this article is expected to be a useful source of information for practitioners, researchers, and decision makers in developing effective IoT strategies and implementations in defense and security systems[5].

II. APPLICATION OF IOT IN DEFENSE AND SECURITY SYSTEMS

A. IoT for Surveillance and Situation Monitoring

One of the main applications of IoT in defense and security systems is surveillance and situation monitoring. Using sensors connected to an IoT network, the system can monitor environmental conditions in real-time and transmit data to the control center for further analysis. This can help decision makers understand the situation and respond quickly in emergency situations.

IoT can monitor the temperature, humidity, and air pressure around military sites or areas to be guarded. The data collected can be used to monitor environmental conditions and ensure troop readiness for operations. IoT can also monitor human and vehicle activity around strategic locations, such as military bases or government buildings. This data can help identify potential threats and improve regional security. The use of IoT in surveillance and situation monitoring can improve system efficiency and accuracy [6]. However, that also points out there are some challenges in integrating IoT sensors into existing systems, such as data security and system interoperability.

B. IoT in Military Sensor Networks

A military sensor network is a collection of sensors connected to a network to collect and transmit data on environmental conditions, enemy movements, and other tactical information in a more integrated and responsive manner. IoT is used to connect sensors located on ships,

airplanes, and ground vehicles into one integrated network. The data collected by the sensors can be transmitted to the control center and processed in real-time to provide accurate information about the situation on the ground.

The use of IoT in military sensor networks can enhance military intelligence capabilities and support more accurate and effective decision-making [7]. However, challenges such as limited battery life and cybersecurity need to be addressed in the development of IoT sensor networks for the military.

C. IoT in Border Monitoring and Regional Security

Border monitoring and securing territories are important tasks in defense and security systems. IoT is used to collect and analyze data from various sensors to identify potential threats and improve border and territory security.

Using sensors connected to an IoT network, border monitoring systems can keep an eye out for suspicious movements and activities along the border. These sensors may include motion sensors, sound sensors, and surveillance cameras that can detect suspicious human or vehicle movements. The data collected by these sensors is then sent to the control center for further analysis and action. The application of IoT in border monitoring and security can provide benefits such as improved early detection, faster response, and reduced risk of human error [8]. However, challenges need to be overcome, such as big data management and analysis, network security, and privacy.

D. IoT for Predictive Maintenance and Asset Management

IoT is applied in predictive maintenance and asset management. In defense and security systems, timely and effective maintenance of equipment and assets is essential to maintain optimal availability and performance.

Using sensors connected to the IoT network, the system can collect real-time data on the condition of equipment and assets. These sensors can monitor temperature, vibration, humidity, and other parameters relevant to the operational condition and reliability of the asset. This collected data can be used to analyze asset performance, detect potential damage or failures, and plan predictive maintenance.

The application of IoT in predictive maintenance and asset management can help in optimizing maintenance, minimizing losses due to downtime, and improving asset usage efficiency [9]. However, challenges such as big data management, integration with existing systems, and information security need to be considered in this IoT implementation.

III. Advantages and Benefits

A. Improved Operations and Oversight Effectiveness

The application of IoT in defense and security systems provides a significant improvement in the effectiveness of operations and surveillance. With a network of connected sensors, information can be collected in real-time and analyzed to better understand the situation. This allows decision makers to have a more comprehensive understanding of the environment and optimize the actions taken [10].

B. Responsiveness and Faster Decision Making

Defense and security systems become more responsive and decisions can be made faster. Data collected in real-time from IoT sensors provide accurate and up-to-date information about environmental conditions, enemy movements, or potential threats. This information allows decision-makers to respond quickly and take appropriate measures in the face of rapidly evolving situations [10].

C. Reduced Operational and Maintanance Costs

The application of IoT can also result in reduced operational and maintenance costs in defense and security systems. Using IoT-based predictive maintenance, military assets can be monitored continuously, allowing maintenance or repair needs to be identified before more serious damage occurs. This reduces sudden repair costs and minimizes unwanted operational downtime and can optimize the use of resources and energy, thereby reducing overall operational costs [11].

Improved Security and Threat Protection The implementation of IoT in defense and security systems can improve security and threat protection. With a network of connected sensors, threats can be detected early through border monitoring, area surveillance, and intrusion detection. The data collected and analyzed by IoT systems provide more accurate information about suspicious activities, enabling more effective prevention and response measures [10].

IV. Challenges and Issues

A. Data security and privacy

Data security risks become higher when data is transmitted over an IoT network. Data security threats can come from cyberattacks, hacking, or hacking. Therefore, data security must be a top priority in the implementation of IoT systems in security and defense. There needs to be an effort to secure data and systems connected to the IoT network as well as protection of confidential or important data sent over the network [12].

B. Interoperability and system integration

Different devices and systems must be able to interact and work together seamlessly. However, interoperability and system integration are often challenges in the application of IoT in defense and security systems. Poorly integrated systems can result in inaccurate or poorly organized data, which can affect the system's ability to make decisions and take necessary actions [13].

C. System network scalability and comlexity

IoT in security and defense consists of thousands of devices connected to a network. The scale and complexity of the network can make network management and maintenance difficult and expensive. Poorly scalable IoT systems can hinder the system's ability to handle large volumes of data and improve system performance [14].

Dependence on network connectivity and availability Network connectivity and availability are important factors in the application of IoT in defense and security systems. If the

network is not available, the IoT system cannot function properly. Reliance on network connectivity and availability can be challenging in emergency situations or during network outages [1].

V. Future Research Directions

A. Development of robust security protocols and standards

The development of strong security protocols and standards is important in the application of IoT in defense and security systems. Protocol design and implementation must be able to protect data, counter cyberattacks, and maintain system integrity. This research can include the development of strong encryption techniques, secure authentication, and effective intrusion detection methods [15].

B. Improved artificial intelligence anda data analytics

Improved artificial intelligence (AI) and data analytics can expand the capabilities of IoT systems in defense and security systems. This research focuses on developing AI algorithms that can analyze sensor data and make decisions automatically. In addition, the use of advanced data analytics can assist in pattern recognition, threat detection, and situation prediction that can improve the response and effectiveness of operations [16].

C. Research on mitigating security risks and threats

Aims to identify and mitigate security risks and threats associated with the application of IoT in defense and security systems. Research focus may include the development of risk mitigation techniques, system vulnerability analysis, and attack response strategies that can protect systems from cyberattacks and other threats [17].

D. Development of a robust IoT platform and architecture

The development of a resilient IoT platform and architecture is important in the application of IoT in defense and security systems. This is related to the design and development of infrastructure that is reliable, scalable, and resistant to attacks. The ultimate goal is to ensure the reliability, speed, and security of IoT networks and good interoperability between connected devices and systems [17].

VI. Conclusion

In this literature review, the application of the Internet of Things (IoT) in defense and security systems offers great potential in improving the effectiveness of operations, surveillance, maintenance, and security in this context. However, there are several challenges that need to be overcome for the application of IoT in defense and security systems to be successful.

Challenges include data security and privacy, interoperability and system integration, network scalability and complexity, and reliance on network connectivity and availability. Overcoming these challenges requires comprehensive efforts in securing data, developing uniform communication standards, designing scalable infrastructure, and considering alternative solutions to overcome dependency on network connectivity.

The proposed research direction is as follows:

1. Development of stronger security solutions: Further research is needed to develop more advanced and reliable security technologies, such as secure data encryption, intelligent cyberattack detection, and strong authentication mechanisms.
2. Improved interoperability: Further research can be conducted to develop uniform communication protocols and open standards, thus facilitating integration between different devices and systems in defense and security systems.
3. Better network scalability: Research should focus on developing a network infrastructure that can handle large volumes of data and can be scaled easily when future device additions occur.
4. Alternative solutions to network connectivity: Research can be directed towards exploring alternative solutions, such as the use of ad hoc networks or resilient mobile network technologies, to overcome the dependency on network connectivity and availability.

By addressing these challenges and steering research in the right direction, the application of IoT in defense and security systems has the potential to deliver significant benefits, improve operational efficiency, and enhance security and protection against existing threats.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/J.COMNET.2010.05.010.

[2] S. Mittal, A. Agrawal, and A. Kumar, “Internet of Things (IoT) and its applications for defense: A Review,” *Def. Sci. J.*, vol. 66, no. 3, pp. 238–247, 2016.

[3] R. Want, B. N. Schilit, and S. Jenson, “Enabling the internet of things,” *Computer (Long. Beach. Calif).*, vol. 48, no. 1, pp. 28–35, Jan. 2015, doi: 10.1109/MC.2015.12.

[4] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, “Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications,” *Sensors 2021, Vol. 21, Page 3654*, vol. 21, no. 11, p. 3654, May 2021, doi: 10.3390/S21113654.

[5] S. Upadhyay, S. Kumar, S. Dutta, A. K. Srivastava, A. K. Mondal, and V. Kaundal, “A comprehensive review on the issues related to the data security of internet of things (IoT) devices,” *Adv. Intell. Syst. Comput.*, vol. 989, pp. 727–734, 2020, doi: 10.1007/978-981-13-8618-3_74/COVER.

[6] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, “A Review on Internet of Things for Defense and Public Safety,” *Sensors 2016, Vol. 16, Page 1644*, vol. 16, no. 10, p. 1644, Oct. 2016, doi: 10.3390/S16101644.

[7] Dublin, “Global Military IoT & Sensors - Market and Technology Forecast to 2028,” 2021. Accessed: May 22, 2023. [Online]. Available: https://www.researchandmarkets.com/reports/5116519/global-military-iot-and-sensors-market-and?utm_source=GNOM&utm_medium=PressRelease&utm_code=qf2xz9&utm_campaign=1557641+-+Global+Military+IoT+%2526+Sensors+Markets+Report+2021-2028%253A+Land%252C+Air%252C+Naval%252.

[8] M. Ahmid and O. Kazar, “A Comprehensive Review of the Internet of Things Security,” *J. Appl. Secur. Res.*, 2021, doi: 10.1080/19361610.2021.1962677.

[9] P. Killeen, B. Ding, I. Kiringa, and T. Yeap, “IoT-based predictive maintenance for fleet management,” *Procedia Comput. Sci.*, vol. 151, pp. 607–613, 2019, doi: 10.1016/J.PROCS.2019.04.184.

[10] A. Heidari and M. A. Jabraeil Jamali, “Internet of Things intrusion detection systems: a comprehensive review and future directions,”

Cluster Comput., pp. 1–28, Oct. 2022, doi: 10.1007/S10586-022-03776-Z/METRICS.

[11] Y. K. Teoh, S. S. Gill, and A. K. Parlikad, "IoT and Fog-Computing-Based Predictive Maintenance Model for Effective Asset Management in Industry 4.0 Using Machine Learning," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2087–2094, Feb. 2023, doi: 10.1109/JIOT.2021.3050441.

[12] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.

[13] E. Lee, Y. D. Seo, S. R. Oh, and Y. G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 2, pp. 1020–1047, Apr. 2021, doi: 10.1109/COMST.2021.3067354.

[14] A. Gupta, R. Christie, and R. Manjula, "Scalability in Internet of Things: Features, Techniques and Research Challenges," *Int. J. Comput. Intell. Res.*, vol. 13, no. 7, pp. 1617–1627, 2017, Accessed: May 23, 2023. [Online]. Available: http://www.ripublication.com.

[15] S. Boukhalfa, M. Tahar, A. Abdelmalek Amine, and R. Mohamed Hamou, "Border Security and Surveillance System Using IoT," *Int. J. Inf. Retr. Res.*, vol. 12, no. 1, pp. 1–21, Jan. 2022, doi: 10.4018/IJIRR.289953.

[16] M. Payal, P. Dixit, T. V. M. Sairam, and N. Goyal, "Robotics, AI, and the IoT in Defense Systems," *AI IoT-Based Intell. Autom. Robot.*, pp. 109–128, Jan. 2021, doi: 10.1002/9781119711230.CH7.

[17] H. S. A. Ahmed, "The Rising Security Risk and Mitigation Options for IoT Devices," 2020. Accessed: May 23, 2023. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-13/the-rising-security-risk-and-mitigation-options-for-iot-devices.