Indonesian Journal of Interdisciplinary Research in Science and Technology (MARCOPOLO)
Vol. 2, No. 5, 2024 : 523 - 530

Building International Cooperation in Utilizing the Internet of Things (Iot) for Defense: Towards Better Global Security

Elga Adestria[1*], Hikmat Zakky Almubaroq[2]
Universitas Pertahanan Republik Indonesia
Corresponding Author: Elga Adestria elga.ades@gmail.com

A R T I C L E I N F O

Keywords: Internet of Things, International Cooperation, Global Security, Defense

Received : 01 April
Revised : 14 April
Accepted: 16 May

A B S T R A C T

The digital Era has a fairly rapid development, in the era of Industry 4.0, the defense industry donated by manufacturing companies is driven by the presence of information and Communication Technology. The Internet of Things (IoT) has become one of the key factors in the transformation of the global industry. This research was conducted using qualitative methods with a literature review approach. The results and analysis are carried out by absorbing various literature such as books, journals, articles, news, online documents, internet related to the research topic which are then extracted, filtered with the aim of evaluating the information based on predetermined criteria. The role of international cooperation in improving IoT security is very complex, it includes several important aspects. First, international cooperation can facilitate the exchange of information about security threats and best practices between countries. With a broad range of knowledge and experience, countries can learn from each other and develop more effective strategies in addressing IoT security risks. Conclusion as of this writing, with international cooperation and strong standardization, companies can prioritize security in IoT implementation to reduce the risk of data breaches and breaches, and create a more secure and trustworthy environment for IoT utilization in a global context.

INTRODUCTION

The digital Era has a fairly rapid development, in the era of Industry 4.0, the defense industry donated by manufacturing companies is driven by the presence of information and Communication Technology. The Internet of Things (IoT) has become one of the key factors in the transformation of the global industry. This phenomenon has penetrated into various sectors, opening the door to unlimited innovation in improving efficiency, productivity, and convenience (Fraga-Lamas et al., 2016). The ability to connect devices, collect data and enable interaction between them has had a significant impact on many sectors. However, with the advancement of technology is also able to bring new challenges, especially in the field of security and Privacy. IoT users themselves have been effectively utilized in various industrial sectors for remote monitoring, surveillance, and decision making, except for the defense sector (Sirait et al., 2023).

A more reliable defense capability will make a country have a global power that will not be underestimated by the countries in the world. The defense industry must have a focus on increasing national needs and also maintaining system security in the defense industry itself. In today's digital era, of course, we are no strangers to data theft, so file security is becoming increasingly important to avoid world crime. The Internet of Things is able to be applied because it is related to technology and programs developed from before (Wasserbauer, 2023). To get the needs in achieving cyber security will be easier if done globally and through collaboration with other countries.

The importance of building international cooperation in the use of IoT for better global security certainly cannot be underestimated, when there are many threat factors, especially in cyber attacks that are increasingly complex, diverse, and spread globally, it will be very important of course to have cross-border collaboration. This cross-border collaboration will be key to mitigating risks and protecting sensitive data infrastructures. Therefore, the company has an important role as a stakeholder to try to maintain the security of important company data. With knowledge, experience and resources, countries and companies can support each other in building a solid foundation for greater global security.

In this context, the study aims to investigate the role of international cooperation in harnessing the potential of IoT to enhance global security, particularly in the context of enterprises. Through a comprehensive approach, this paper is expected to identify strategies and best practices that can be applied to face complex security challenges in the IoT environment.

LITERATURE REVIEW

Introduce of Internet of Things (IoT)

The Internet of Things was introduced by Kevin Ashton in 1999. Kevin is a British technology pioneer, he introduced IoT for the first time when he worked at the Massachusetts Institute of Technology (MIT) Auto-ID Center. But only then there is) is a concept that refers to the connectivity between various physical devices through the internet. The basic concept of IoT involves devices equipped with sensors, software, and an internet connection, allowing them to collect data,

share information, and even perform certain actions based on the data they acquire.

The Internet of Things (IoT) is a concept in which physical objects are connected to the internet and can communicate with each other without human intervention. This concept has transformed the information technology landscape and provides new opportunities to improve efficiency and productivity in various sectors, including in the context of the company. In the enterprise context, IoT implementation has brought about a major transformation in supply chain management, asset monitoring, and real-time data analytics. Enterprises can leverage sensors and connected devices to collect relevant data from the physical environment, providing deeper insights for more strategic decision-making. However, each of its benefits carries significant security risks. For example, an increase in the number of connected devices increases the vulnerability of potential attacks to cybercrime, making IoT security less secure (Atzori et al., 2010). The impact of the power of IoT has a considerable influence on several aspects. The Internet of Things currently has appeal and attention for all its users with a view to a better global infrastructure. Connectivity that can be generated anywhere, anytime, and by anyone.

The following are key elements in the IoT ecosystem according to (Sokolovi & Marković, 2023):

1. **IoT devices**: these are physical objects such as sensors, cameras, measuring devices, or other smart devices that are connected to the internet and equipped with the ability to send and receive data.
2. **Network**: a network is an infrastructure that allows IoT devices to connect with each other and with servers or other systems. These can be wired networks, wireless networks (such as Wi-Fi, Bluetooth, or cellular networks), or even satellite networks.
3. **Data processing:** The Data collected by IoT devices must be processed to obtain useful information. This can be done on the device itself (edge computing) or on a server or cloud.
4. **Management:** this involves managing and regulating IoT devices, as well as the security and privacy of the data collected by them.
5. **Application**: an application or solution that uses data collected by an IoT device to deliver a specific service or solution. Examples include environmental monitoring systems, smart homes, autonomous vehicles, and more.

In this modern era, the Internet of Things (IoT) has become very relevant in all fields including the defense sector. The use of IoT is making great progress towards monitoring and maintaining military assets. This helps improve operational efficiency, such as extending the life of military equipment, reducing costs and risks due to failures in the field. In terms of logistics and inventory management in the defense sector, it can help track and manage supplies efficiently, thereby reducing shortages in military operations. Overall, the relationship between the internet of Things and the defense sector has opened the door to a new era in national defense capabilities. By effectively harnessing

the potential of IoT while addressing the Associated security challenges, the military can take a major step towards progress and excellence in national defense.

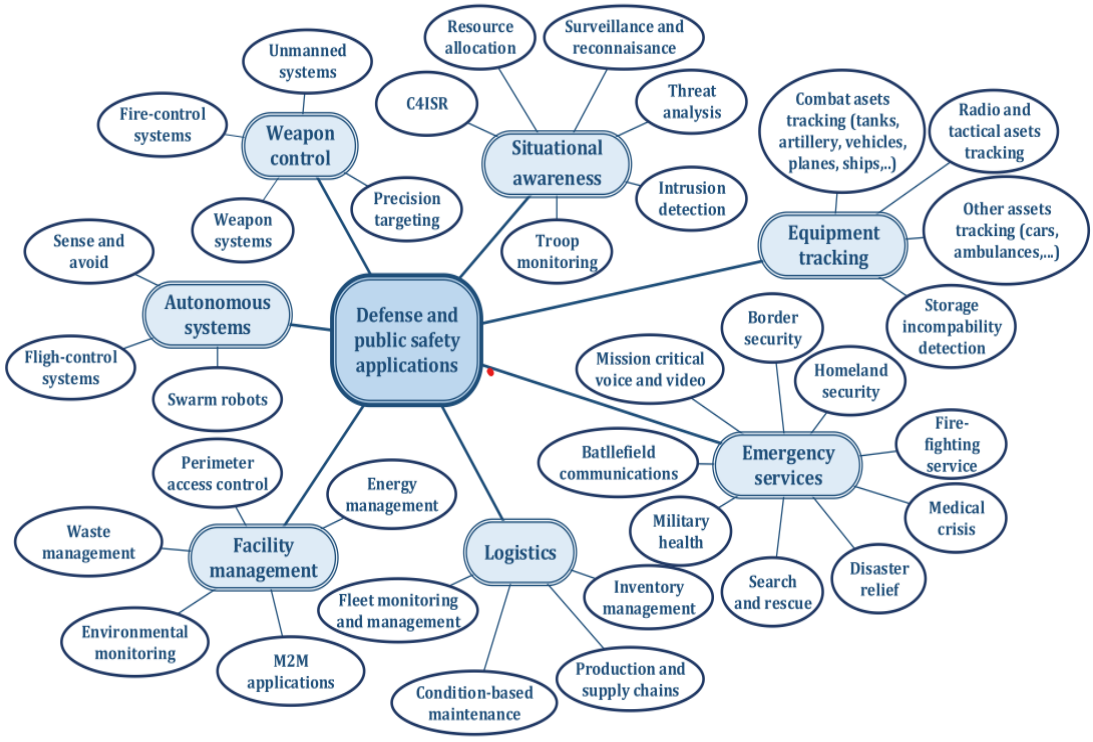

Figure 1. The Main Application Areas of IoT Technology in Defense and Public Safety Sectors (Sokolovi & Marković, 2023)

Security Challenges in The Use of IoT in the Company

Although the potential benefits of implementing IoT are quite good, it is also important for companies to face a number of resulting security challenges. In the midst of a changing digital paradigm, where devices are constantly connected, the need to maintain information and operational security is more important than ever. Security challenges in the use of the Internet of Things (IoT) in the company is a crucial issue that needs to be understood in depth. One of the most common challenges today is data security. Data generated by IoT devices is often very sensitive and confidential, making it vulnerable to theft or manipulation by parties who do not have an interest in the data. In addition, the long life span of IoT devices often makes them vulnerable to data security attacks that can occur from time to time. Another challenge is the vulnerability of IoT devices to cyber attacks, especially because many devices do not have adequate security systems. This can lead to significant risks for the company, including loss of important data, operational disruptions, and financial losses (Al-Fuqaha et al., 2015)

Implementation of Global Policies and Standards

Global policies and standards are quite important given the need for collaborative utilization of IoT in the company. The implementation of global

policies and standards in the context of the Internet of Things (IoT) is essential to strengthen security and interoperability on an international scale . Cohesive global policies can help address cross-border security challenges (Mahmoud et al., 2016). With a clear framework in place, countries can easily collaborate and develop common guidelines related to data privacy and the use of the Internet of Things. This policy should cover all aspects such as data privacy, encryption, authentication, and emergency measures in the face of cyber attacks. Clear and universally accepted security standards help companies to have clear guidance in implementing effective security practices and complying with applicable regulations. With clear policies and backups in place, companies will be able to prioritize security in the development and implementation of their IoT deployments, thereby reducing the risk of attacks and data breaches (Zanella et al., 2014).

Collaboration Between Government and Private Sector

Close cooperation between the government and the private sector is also an important component in efforts to improve IoT security. These partnerships can include the exchange of resources, investment in security research and development, and the establishment of relevant regulatory bodies. Governments have a role to play in formulating policies and regulations that support IoT security, provide the infrastructure needed to manage security risks, and incentivise companies to improve IoT security in their operations, while providing direct insight into the challenges and needs faced in securing their IoT infrastructure and providing knowledge and resources to help develop more innovative and efficient security solutions. Collaboration between the government and the private sector can create a more secure environment for the utilization and use of IoT in enterprises, and is expected to reduce the risk of cyber attacks and protect sensitive data (Sirait et al., 2023).

METHODOLOGY

This research was conducted using qualitative methods with a literature review approach. The results and analysis are carried out by absorbing various literature such as books, journals, articles, news, online documents, internet related to the research topic which are then extracted, filtered with the aim of evaluating the information based on predetermined criteria.

RESEARCH RESULT AND DISCUSSION

The role of International Cooperation in improving the security of the Internet of Things (IoT)

The role of international cooperation in improving IoT security is very complex, it includes several important aspects. First, international cooperation can facilitate the exchange of information about security threats and best practices between countries. With a broad range of knowledge and experience, countries can learn from each other and develop more effective strategies in addressing IoT security risks. In addition, international cooperation can also help in the development of global security standards for IoT devices and networks. With the existence of diverse standards, companies can ensure that IoT products

used meet certain security requirements, regardless of the country of origin of the manufacturer. This can increase trust and reduce vulnerability to attacks.

International cooperation in the context of IoT security is key to creating a secure and trustworthy environment for companies moving globally. Through cross-country cooperation will be able to facilitate the exchange of best practices in securing IoT infrastructure or "Sharing Best Practices". Sharing Best Practices refers to collaborative practices in which entities or organizations share experiences, knowledge, and best practices in a particular field. In the context of Internet of Things (IoT) security for enterprises, sharing best practices enables companies, governments, and other institutions to learn from each other about effective strategies, techniques, and tactics in addressing security risks associated with IoT. This is especially important because IoT security threats will continue to evolve over time, and with a wide range of knowledge and experience, entities can identify more innovative and efficient solutions. Sharing Best Practices also allows entities to avoid mistakes made by others and adopt the best approach to managing IoT security (Khan et al., 2022).

In order to strengthen security in the implementation of the Internet of Things, standardization is necessary, which refers to the process of developing and implementing standards that are consistent and uniform. In the context of IoT, standardization is very important because it can help ensure that IoT service products meet certain security requirements set by standards agencies. With clear and standardized standards, companies can ensure that the IoT products used meet the expected level of security. In addition, standardization also supports interoperability between IoT devices from different manufacturers, enabling smoother integrity between devices and systems, which is ultimately expected to strengthen overall security. Standardization is therefore key in creating a secure, reliable and trustworthy IoT environment.

CONCLUSIONS AND RECOMMENDATIONS

From the discussion that has been delivered, it can be concluded that the role of international cooperation in improving the international security of Things (IoT) for companies is very important. This cooperation involves several key aspects, including the exchange of information on security threats and best practices between countries, as well as the development of global security standards for IoT devices and networks. First of all, the exchange of information and best practices allows countries to learn from each other and develop more effective strategies in addressing IoT security risks. In addition, standardization plays an important role in ensuring that IoT products and services meet certain security requirements set by standards agencies, as well as facilitating interoperability between IoT devices from different manufacturers. With international cooperation and strong standardization, companies can prioritize security in IoT implementation by reducing the risk of data breaches and breaches, and creating a more secure and trustworthy environment for IoT utilization in a global context.

ADVANCED RESEARCH

In writing this article the researcher realizes that there are still many shortcomings in terms of language, writing, and form of presentation considering the limited knowledge and abilities of the researchers themselves. Therefore, for the perfection of the article, the researcher expects constructive criticism and suggestions from various parties.

REFERENCES

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors (Basel, Switzerland)*, *16*(10), 1–44. https://doi.org/10.3390/s16101644

Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in Internet of Things: A Review. *IEEE Access*, *10*, 104649–104670. https://doi.org/10.1109/ACCESS.2022.3209355

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, *December 2015*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

Sirait, J., Alrasyid, H., & Soraya, N. A. (2023). Strengthening The Defense Industry's Independence Through The Internet Of Things In The Manufacturing Sector: A Review. *International Journal of Science, Technology & Management*, *4*(2), 335–340. https://doi.org/10.46729/ijstm.v4i2.764

Sokolovi, V. S., & Marković, G. B. (2023). *Internet of Things in military applications*. *71*(4), 1148–1171. https://doi.org/10.5937/vojtehg71-46785

Wasserbauer, M. (2023). The Effect of Information Technology Infrastructure and the Internet of Things on Defense Industry Management Information Systems. *Dinasti International Journal of Digital Business Management*, *4*(1), 190–201. https://doi.org/10.31933/dijdbm.v4i1.1925

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

https://it.telkomuniversity.ac.id/internet-of-things-pengertian-sejarah-kelebihan-dan-kekurangannya/

https://el.iti.ac.id/pengantar-apa-itu-internet-of-things-iot/