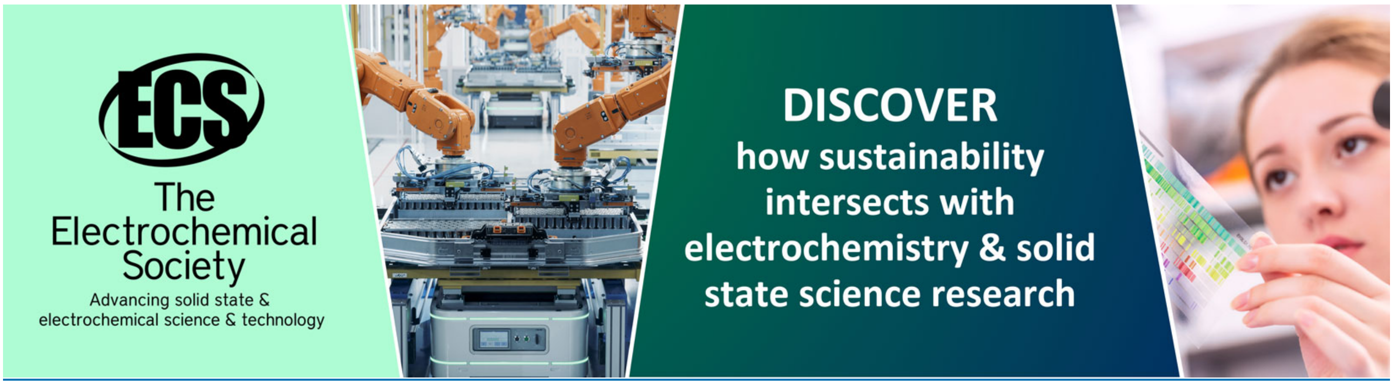
IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

# Internet of Things Cyber Security in Digital Era



# Internet of Things Cyber Security in Digital Era

**M Solihat[*], R V Wulansari**

Departemen Ilmu Komunikasi, Universitas Komputer Indonesia, Indonesia

Email: *manap.solihat@email.unikom.ac.id

**Abstract.** This study aims to determine cybersecurity security in terms of data transfer in the digital era. This study used a descriptive qualitative approach, namely a literature study. The results of this study are to show that using the internet remains safe and avoids dangerous things. With the positive influence of digital technology on cybersecurity, it can be concluded that cybersecurity is to maintain security from technological crimes. This research is expected to serve as a warning to the public to be careful in using the internet.

## 1. Introduction

Cybersecurity is important because it can protect corporate and personal data. All companies with digital-based data are highly recommended to pay attention to and use cybersecurity when storing, accessing, and retrieving important information. Studying technology security demonstrates the need for new conceptual and analytical resources and cybersecurity research aimed at the technical and social intersection [1]. Technology security nowadays is not just a technical issue. Lithuanian Cybersecurity Law defines cybersecurity as a tool for legal action. The dissemination of technical and organizational information needs to be taken to detect, analyze, prevent, and respond to a problem in technology. It is described as an activity or event that may cause unauthorized access to the system communication and information, electronic communication networks. It is also described as control systems for electronic communication network processes or industrial processes that control operations to destroy, delete, destroy, or modify electronic information and restrict access to electronic information. It also modifies electronic information, restricts, or withdraws access to electronic information. Moreover, it is possible to use non-public information in electronic format by an unauthorized person. The main objective is to provide fast recovery from electronic communication networks, information systems, or industrial process control systems in the event of a cyber-problem or cyber-attack [2].

Identity theft allows data theft to occur, but it is a potentially more serious nuisance. Thus, victims due to data theft are being forced to change a new password. The more important data that can be stolen, the more difficult it is to prove its identity. It will also take time to recreate the documentation [3]. Security and protection in cyberspace must be improved regarding critical information infrastructure, which is very important for every country's safety and economic welfare. Security of internet users has become an essential aspect of developing new technologies and public policies. Cybercrime must be eradicated safely. Since using technical measures alone cannot prevent crime, effective investigation and prosecution of cybercrime by a law enforcement agency is essential. Many countries and governments are currently enforcing strict cyber securities laws to avoid the loss of important information. People must be trained in cybersecurity to be free from crimes from cyberspace [4].

Cybersecurity is protection connected to the internet, including hardware, software, and data from cyber-attacks. The Arizona Cyber Talent Organization states that cybersecurity is the protection of IT systems [5]. Maintaining cybersecurity is to be able to test and provide developing implementations and implement strategies and report every incident so that it can be prepared to act and track the status of network security. Security techniques in technology must solve problems that endanger technology to overcome cybersecurity [6]. The definition of security is a process to protect physical objects against damage, loss, or unauthorized access to maintain the confidentiality and integrity of information about things and to make object information available regardless of time [7].

Security technology implementation is an option and attempts to protect information assets from network attacks or threats or information systems. Currently, technologies present many securities as a security protection for attacks or threats to information networks. Nowadays, many security technologies present as a security protection for attacks or threats to information networks or systems, including cryptographic systems, IDS, SSL, firewalls, IPSec, antivirus systems, authentication, and others [8]. There is no longer any way to place cyber, and it cannot be treated separately from real-world security. If we look to the reality that society's progressive information is taking place, the number of devices connected to the internet also increases.

It is realistic to expect the emergence of new scenarios that violate individual, corporate, national, and global security. The most fundamental problem is that cyberculture is developed faster than cybersecurity, which further implies that cyberspace is integrally at a specific risk [9]. In Indonesia, cyber can still increase. In addition, the number of internet users in Indonesia is still not evenly distributed because there are still many who cannot use internet devices properly, so that cyber law in Indonesia cannot be implemented. Therefore, Indonesia establishes strategic steps to determine cybersecurity and policy based on the National Security for Homeland Security consistency, the US guideline in overcoming various cyber threats to existing infrastructure, and recovering damage caused by cyber-attacks.

Threats and security attacks on social media have been discussed in the previous research. Moreover, based on that research, we must continually protect and secure our data as social media users. In this research, we aim at providing education to be more careful in using technology in the digital era.

## 2. Method

This research used a descriptive qualitative method, namely the literature study approach. Later, we will see some of the previous research will be used as a reference regarding cybersecurity in the Digital Age, where crimes on the internet are increasingly facilitated, and security in the world of technology is increasingly being threatened. Therefore, cybersecurity must become the center of technological attention in the current era then look for valid and accurate data regarding cybersecurity. With proper and precise data, hopefully, this research is developing according to the need and can be used as learning material about cybersecurity

.

## 3. Results and Discussion

### *3.1 Results*

Crime in IoT can occur through anything with various devices. Moreover, every crime can occur. Table 1 shows the crimes on IoT.

**Table 1.** Crimes in the IoT

| **No** | **Source** | **Devices** | **Cybercrime in the IoT** |
|---|---|---|---|
| 1. | Network | Wireless network router, access points, sensor network | Unauthorized access and data modification |
| 2. | Network parameter devices | Firewalls, servers | Unauthorized access |
| 3. | Web | Web servers, web clients, and social networks | Copyright or intellectual property infringement, cyber defamation |
| 4. | Cloud | Cloud systems | Data theft |
| 5. | End nodes | Game consoles, mobile devices, smart TV's, readers | Distribution of malware, data theft, spamming |

From the crimes in the IoT based on Table 1, there are several ways to carry out the required security action on the system to minimize crimes in the IoT. Table 2 shows a list of security requirements that are needed for the system in general.

**Table 2.** General security requirements for the IoT

| No | Requirement | Description |
|---|---|---|
| 1. | Resilience to attacks | To avoid a single point of failure, the system must adapt itself to the failure node |
| 2. | Data authentication | Data and objects that have been retrieved must be authenticated |
| 3. | Access control | From the data provided, the information provided should be able to implement access controls |
| 4. | Client privacy | The system can maintain the privacy of the information provider or client data to provide security and convenience for customers |
| 5. | User identification | Before using users to use the system, they must perform a validation process |
| 6. | Secure storage | Data that has been stored on the system must be kept confidential and ensure the integrity of sensitive information |
| 7. | Identity management | Link user rights and user restrictions to the system to identify individuals/things in the design and control their access to the system |
| 8. | Secure data communication | Ensure the confidentiality and integrity of data communicated by authenticating peer-to-peer communications and preventing rejection of communication transactions, and protecting the identity of communicating entities |
| 9. | Availability | Denial of access or use of user authorization from unauthorized persons or systems |
| 10. | Secure network access | Only authorized devices can provide a network connection or service access |
| 11. | Secure content | Protect the rights of digital content used in the system with Digital Rights Management (DRM) |
| 12. | Secure execution environment | To protect against malicious applications, it is necessary to implement a secure, managed-code, runtime environment designed |
| 13. | Tamper resistance | When the device falls into the hands of malicious parties, then maintain security requirements and check logically |

### *3.2 Discussion*

If there has been a crime in the IoT, a forensic investigation must be carried out. The forensic analysis uses science and technology to investigate and establish a criminal or civil court [11]. Forensic investigations aim to carry out experiments to find facts and create the truth of an incident. The greatest challenge for computer forensics is developing methods and providing validation of the techniques, which can be used to produce tangible and reliable evidence to protect against harm [12]. IoT poses challenges to forensic researchers. These challenges are when the crime of spreading data has widened, the lines between networks are blurred, and the privacy of users with personal networks is increasingly fading. Then, it becomes non-private, and private networks become public networks. There are differences when doing traditional and IoT digital forensic investigations. Table 3 shows a traditional digital forensic investigation.

**Table 3.** Traditional digital forensics investigations

| No | Criterion | Traditional digital forensics investigations |
|---|---|---|
| 1. | Speed of response to incident | Conduct investigation when new events occur |
| 2. | Variety of evidence sources and types | There is sufficiently measured and extensive evidence |
| 3. | Frameworks adaptable | There is a possibility |
| 4. | User input | The perpetrator or victim is usually the user - does no play a role in the investigation |
| 5. | Evidence sources | PC, cloud, web clients, mobile devices, social network |
| 6. | Jurisdiction | Government, company, society, individual, social network |
| 7. | Number of devices | There are billions of devices |
| 8. | Types of evidence | Standard files format and electronic documents |
| 9. | Types of network | Wi-Fi, wireless internet, wired, Bluetooth networks, mobile communications |
| 10. | Quality and type of data and evidence | Up to terabytes of data |
| 11. | Protocols | Wireless, IPv4, IPv6, Ethernet, and Bluetooth |
| 12. | What to seize | As required |
| 13. | Ownership | Governments, companies, individuals, groups |

| | | |
|---|---|---|
| 14. | Network boundaries | Relatively clear boundaries s |

Then, the IoT digital forensic investigation is shown in Table 4.

**Table 4.** IoT digital forensics investigations

| No | Criterion | IoT digital forensics investigations |
|---|---|---|
| 1. | Speed of response to an incident | Quite a long response |
| 2. | Variety of evidence sources and types | Sources and evidence that have a more comprehensive range |
| 3. | Frameworks adaptable | Needs frameworks adaptable |
| 4. | User input | Users must remain active using personal IoT, forensic surveillance by the use of adaptable |
| 5. | Evidence sources | Readers, embedded systems sensor nodes, sensor networks, medical implants in humans and animals, other IoTware |
| 6. | Jurisdiction | Government, company, society, individual, social networks |
| 7. | Number of devices | From 50 billion to trillions of devices |
| 8. | Types of evidence | Allows all formats |
| 9. | Types of networks | Sensor network, sensor to reader and vice versa, RFID |
| 10. | Quantity and type of data as well as evidence | Up to exabyte of data |
| 11. | Protocols | RFID |
| 12. | What to seize | Identify the best thing for the source the following evidence |
| 13. | Ownership | Governments, companies, individuals, groups |
| 14 | Network boundaries | Boundary lines that have no clarity |

With the challenges in carrying out digital forensic investigations on IoT, data security on IoT is much needed; it meets the system's general security requirements that users will use. It meets the general conditions of security on the design and can also guarantee user data confidentiality.

## 4. Conclusion

Technological development can make it easier for people to get information quickly. The threats and attacks on technology nowadays are being the most worrying things. In this digital era, it is necessary for us to always be careful in protecting all data because many crimes are committed in any way. Along with the development of technology, the threats will also get heavier. Therefore, there is a need for security to safeguard data.

## Acknowledgment

We want to thank Prof. Dr. Ir. H. Eddy Soeryanto Soegoto, MT as a lecturer in Entrepreneurship in the Field of Information Systems and Communication at Universitas Komputer Indonesia, who has provided knowledge and insight for this research.

## References

[1] Liebetrau, T., & Christensen, KK 2020. The ontological politics of cybersecurity: Emerging agencies, actors, sites, and spaces. *European Journal of International Security*, pp. 1-19.

[2] Limba, T., Plėta, T., Agafonov, K., & Damkus, M. 2019. Cybersecurity management model for critical infrastructure.

[3] Arlitsch, K., & Edelman, A. 2014. Staying safe: Cyber security for people and organizations.*Journal of Library Administration*, **54**(1), 46-56.

[4] Iqbal, H., Al-Utaibi, G., & Bohra, O. P. The Reality of Technologies for Cybersecurity Challenges.

[5] Morantz, B. Cyber Security Is an Application of Decision Sciences.

[6] Callen, J., & James, J., E. 2020. Cybersecurity Engineering: The Growing Need. *Issues in Information Systems*, **21**(4).

[7] Abomhara, M., & Køien, GM 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pp. 65-88.

[8] Bustami, A., & Bahri, S. 2020. Threats, Attacks and Protection Measures on Network or Information System Security: Systematic Review. *UNISTEK*, **7**(2), pp. 59-70.

[9] Mihailović, A., & Rašović, N. Cybersecurity in the New Reality: Systematic Review in the Context of COVID-19.

[10] Simbolon, IS 2017. Cyber Initiatives in the Context of Cybersecurity in the Philippines.*Asymmetric Warfare*, **3**(2).

[11] Philipp, A., Cowen, D., & Davis, C. 2009. *Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions*. McGraw Hill Professional.

[12] Noblett, M. G., Pollitt, M. M., & Presley, L. A. 2000. Recovering and examining computer forensic evidence. *Forensic Science Communications*, **2**(4).