# ETHICS IN INTERNET OF THINGS: CHALLENGES AND OPPORTUNITIES

**Sabina Szymoniak, Mariusz Kubanek**

Department of Computer Science, Czestochowa University of Technology, Poland

sabina.szymoniak@icis.pcz.pl; mariusz.kubanek@icis.pcz.pl

## EXTENDED ABSTRACT

The Internet of Things (IoT) is a network of connected physical devices. Devices exchange data between them using the Internet. IoT is the concept that connects different devices like home appliances, vehicles, sensors or smartphones to the internet network. IoT devices and connections exist in many areas (Szymoniak & Kesar, 2022). We utilize smart washing machines, TVs, and light bulbs. Thus, we can discover IoT gadgets in our daily lives. These gadgets use the proper sensors to regulate a building's lighting or water heating intelligently. With the aid of tracking gadgets, they can also safeguard our security (Khan et al., 2022; Alsaeed & Nadeem, 2022). Devices used in medical IoT assist in managing the critical functions of patients with chronic illnesses, testing blood glucose levels in people with diabetes, alerting doctors when a patient needs medication, and promptly delivering it to the patient (Singh et al., 2022). One of the common uses for IoT in the sector is to warn people about the potential for an earthquake (Sivakumar et al., 2022). In order to avoid potentially fatal scenarios, athletes might use IoT to regulate vital processes and performance (Zhou et al., 2021).

As mentioned, IoT devices use the Internet to communicate. Basically, they use wireless data transmission, for example, WiFi, and LTE / 5G, as secure channels supported by secure cryptographic protocols like SSL/TLS. However, IoT connections also implement and realize other security protocols specially designed for these solutions in the specific solutions. The security protocols define the order in which messages must be sent. We can indicate many security protocols dedicated to different solutions, for example, in medicine or healthcare (Rasslan et al., 2022), (Masud et al., 2022), in fog or edge processing (Pardeshi et al., 2022), for industry (Yi et al., 2022), for meetings (Szymoniak & Siedlecka-Lamch, 2022) or suitable for many domains (Yan et al., 2022).

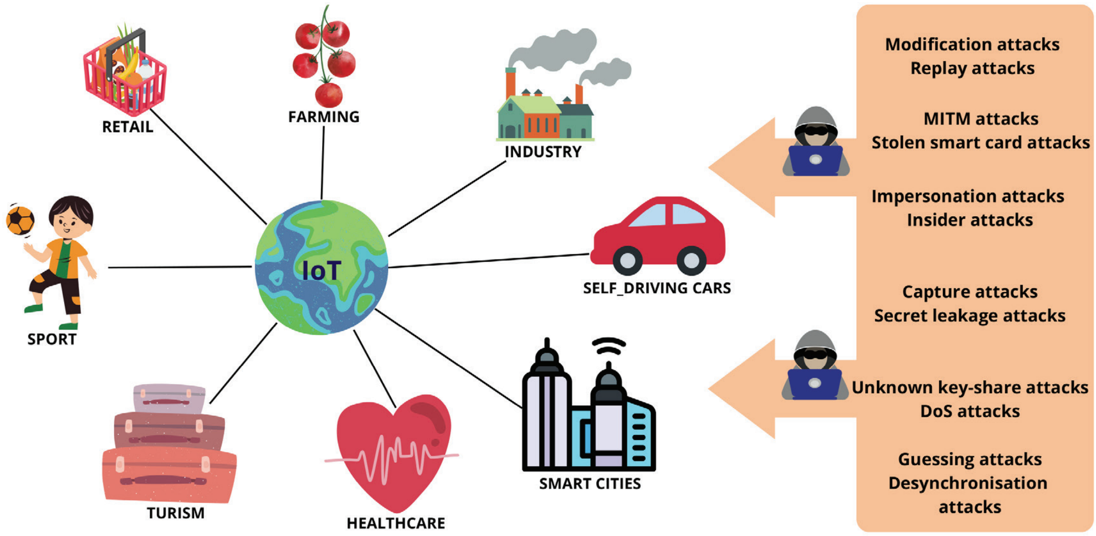
Depending on the protocol's application, we send many different data during communication between devices. Each security protocol should implement the so-called CIA triad, the basic IT security concept. CIA triad ensures the protection of information. Achieving a balance between its three goals is crucial to effectively securing systems and data. CIA triad goals are confidentiality, integrity and availability. Confidentiality ensures that information will be available only to authorized users and protects against unauthorized access. The integrity ensures that data will be accurate, unaltered and undamaged and prevent data modifications or deletions by unauthorized users. The availability ensures that information is available for users at the requested time when they want it. Using backup resources and appropriate hardware safeguards improves availability (Szymoniak & Kesar, 2022).

Also, the security protocols should satisfy some security features. The first is mutual authentication, which refers to two users verifying their authority over each other. User anonymity provides that the user’s authority will be anonymous or hidden. Next, the perfect forward secrecy ensures that even if a private key is compromised in the future, previously mentioned secret keys will not be exposed or compromised. The perfect backward secrecy ensures that even the private keys have been compromised in the past and does not allow previous sessions to be compromised. The last security feature is untraceability. This feature ensures that activities or transactions cannot be traced back to a specific user ((Szymoniak & Kesar, 2022), (Kubanek et al., 2022)).

Unfortunately, the security protocols, even if they fulfil these features, can be vulnerable to many attacks by malicious users ((Szymoniak et al., 2017), (Szymoniak et al., 2018)). From many statistics, there are more than 2000 cyberattacks per day. The attackers search for vulnerabilities in such systems and try to break into them. The system hacking effects are hazardous for many reasons. First, the users can lose their devices because the attacker obtains control of them. Next, he can try to eavesdrop on whole communication in the network and steal private data, logins or passwords. Moreover, the attacker can take control of other devices in the network or the whole Smart Home. Figure 1 summarises IoT solutions and typical cyberattacks on IoT systems.

The cyberattacks' influence on users and their data upon IoT systems entails the ethical consideration of communication on such systems. We must think about the ethics of data storage, which answers questions like what data can be stored, what data should not be stored, and what is the maximum time necessary for sensitive data storage. It is necessary because stored data can be stolen from devices or servers and used. Also, we must consider the risk of data leakage from IoT systems. Moreover, in the case of security protocols, we must investigate how they deal with mentioned security features, what communication elements make vulnerabilities, and how to protect IoT systems and their users against cyberattacks. This paper will consider the challenges and opportunities of ethics in the Internet of Things systems.

Figure 1. IoT solutions and typical cyberattacks on IoT systems.



**KEYWORDS:** Internet of Things, ethics, security, attacks, vulnerabilities.

## REFERENCES

Alsaeed, N. H., & Nadeem, F. (2022). Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues. *Applied Sciences*, *12*(15), 7487. https://doi.org/10.3390/app12157487

Khan, F., Xu, Z., Sun, J., Khan, F. H., Ahmed, A., & Zhao, Y. (2022). Recent Advances in Sensors for Fire Detection. *Sensors*, *22*(9), 3310. https://doi.org/10.3390/s22093310

Kubanek, M., Bobulski, J., & Karbowiak, Ł. (2022). Intelligent Identity Authentication, Using Face and Behavior Analysis. *ETHICOMP 2022*, 42.

Masud, M., Gaba, G. S., Kumar, P., & Gurtov, A. (2022). A user-centric privacy-preserving authentication protocol for IoT-AmI environments. *Computer Communications*, *196*, 45-54. https://doi.org/10.1016/j.comcom.2022.09.021

Pardeshi, M. S., Sheu, R., & Yuan, S. (2022). Hash-Chain Fog/Edge: A Mode-Based Hash-Chain for Secured Mutual Authentication Protocol Using Zero-Knowledge Proofs in Fog/Edge. *Sensors*, *22*(2), 607. https://doi.org/10.3390/s22020607

Rasslan, M., Nasreldin, M., & Aslan, H. K. (2022). Ibn Sina: A patient privacy-preserving authentication protocol in medical internet of things. *Computers & Security*, *119*, 102753. https://doi.org/10.1016/j.cose.2022.102753

Singh, S., Nandan, A. S., Sikka, G., Malik, A., & Vidyarthi, A. (2022). A secure energy-efficient routing protocol for disease data transmission using IoMT. *Computers & Electrical Engineering*, *101*, 108113. https://doi.org/10.1016/j.compeleceng.2022.108113

Sivakumar, P., Sandhya Devi, R.S., Ashwin, M., Rajan Singaravel, M.M. & Buvanesswaran, A.D. (2022). Protocol Design for Earthquake Alert and Evacuation in Smart Buildings. In: Rani, S., Sai, V., Maheswar, R. (eds) IoT and WSN based Smart Cities: A Machine Learning Perspective. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-84182-9_1

Szymoniak, S., & Kesar, S. (2022). Key Agreement and Authentication Protocols in the Internet of Things: A Survey. *Applied Sciences*, *13*(1), 404. https://doi.org/10.3390/app13010404

Szymoniak, S., & Siedlecka-Lamch, O. (2022). Securing Meetings in D2D IoT Systems. *ETHICOMP 2022*, 31.

Szymoniak, S., Siedlecka-Lamch, O., & Kurkowski, M. (2017). Timed analysis of security protocols. In *Information Systems Architecture and Technology: Proceedings of 37th International Conference on Information Systems Architecture and Technology–ISAT 2016–Part II* (pp. 53-63). Springer International Publishing.

Szymoniak, S., Siedlecka-Lamch, O., & Kurkowski, M. (2018). On some time aspects in security protocols analysis. In *Computer Networks: 25th International Conference, CN 2018, Gliwice, Poland, June 19-22, 2018, Proceedings 25* (pp. 344-356). Springer International Publishing.

Yan, D., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. (2022). A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT. *Security and Communication Networks*, *2022*, 1-15. https://doi.org/10.1155/2022/9686049

Yi, F., Zhang, L., Xu, L., Yang, S., Lu, Y., & Zhao, D. (2022). WSNEAP: An Efficient Authentication Protocol for IIoT-Oriented Wireless Sensor Networks. *Sensors*, *22*(19), 7413. https://doi.org/10.3390/s22197413

Zhou, H., Wang, Z., Zhao, W., Tong, X., Jin, X., Zhang, X., Yu, Y., Liu, H., Ma, Y., Li, S., & Chen, W. (2021). Robust and sensitive pressure/strain sensors from solution processable composite hydrogels enhanced by hollow-structured conducting polymers. *Chemical Engineering Journal*, *403*, 126307. https://doi.org/10.1016/j.cej.2020.126307