THEORETICAL FRAMEWORK USING AI: IMPROVING SERVICES WITHIN SMART CITIES

Sabina Szymoniak, Shalini Kesar

Czestochowa University of Technology (Poland), Southern Utah University (USA)

sabina.szymoniak@icis.pcz.pl; kesar@suu.edu

EXTENDED ABSTRACT

This paper is part of an on-going collaborative research to develop a framework that will support notifying emergency services within smart cities ((Joshi et al., 2016), (Tura et al., 2022)). The framework is designed to provide a support system for existing emergency services like ambulances within the city. After reviewing the challenges of the existing frameworks linked with artificial intelligence, the authors propose a theoretical framework using AI that overcomes the existing challenges to provide an efficient mechanism for ambulance services within smart cities. The collaborative work of the authors, experts in risk management and security of computer systems, will provide a significant contribution in the research area that combines best practices of cybersecurity and smart cities. Given that smart cities are increasingly becoming popular in urban areas, this framework, an on-going research, can be a starting point for many services that can help in mitigating, minimising, managing as well as transferring risks when it comes to human life.

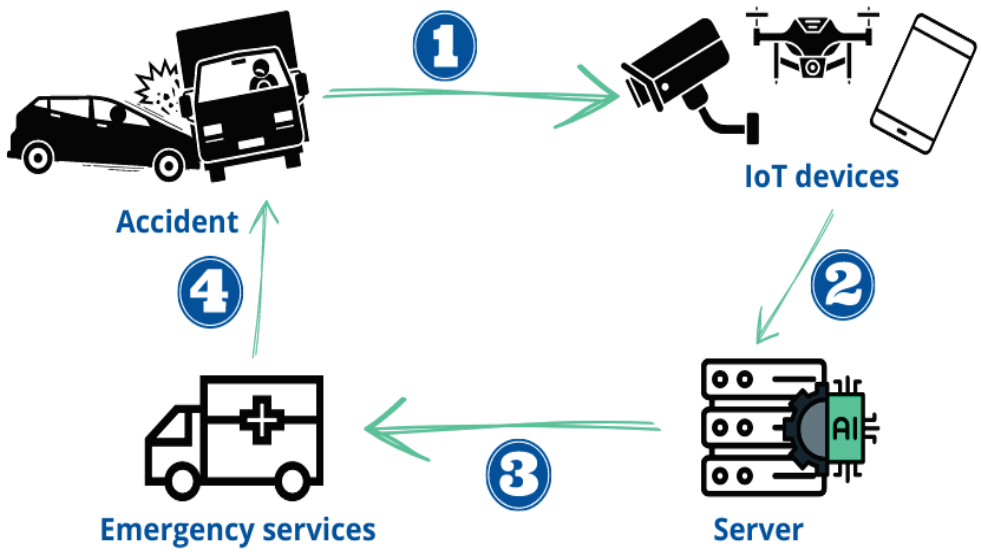
Our daily lives cannot function without smart devices. We employ a variety of gadgets, like intelligent refrigerators, vacuum cleaners, and ovens, to carry out preprogrammed tasks automatically and share data. These gadgets are controlled by smartphones, various sensors, and software that enables us to manage a working environment and carry out particular tasks without human participation. Using such gadgets, we can control our home from anywhere globally, maintaining the right room temperature and ensuring their security. Such devices belong to the Internet of Things, IoT for short. Moreover, they can be used for many more advanced tasks connected with human safety, especially when they are equipped with Artificial Intelligence (AI) methods (("Internet of Things," 2022), (Szymoniak & Kesar, 2022)).

Dependency on data and technology in smart cities will continue to increase. A recent article in IT Magazine (2023) states that data by smart cities is expected to grow by more than 140% between 2023 and 2027. More so, there will be more cellular connections in the Internet of Things projects in smart cities, which are expected to increase at a compound annual rate of 17.9% between 2022 and 2027, reaching a plateau of more than 122 million, with particularly high growth in the next two years. As a result, there will also be more risks from data breaches to fatal accidents on the road to minimise, manage, mitigate as well transfer risks, rescue services dependency will increase to help the injured and secure the area around the incident. Also, city dwellers can witness situations that may turn into dangerous situations, for example, when a group of people argue. In some cases, the argument may turn into a fight.

This paper proposes a proof of concept as a framework (see Figure 1 below) that focuses on using a network of IoT devices as an intelligent system to support ambulance services, which can minimise fatality. As shown below, smart devices equipped with a camera can capture the

moment of an accident or other dangerous situation and then send photos to a trusted server equipped with AI-based software to recognise the situation type, decide if the situation is dangerous, and notify the rescue services.

Figure 1. The architecture of the proposed system.



As mentioned earlier, Figure 1 shows the proposed system's architecture, which consists of four ingredients. The first is the scene of a dangerous situation, like an accident. The second is the network of IoT devices. The third is the trusted server equipped with the appropriate software. The last ingredient is the rescue services. The operation of the system will be a continuous, four-step process. The situation happens in the first step, and the IoT device takes this event's photo. Next, the device sends the captured photo to the trusted server via the Internet (step 2). After that, the server will process the obtained photos using AI-based software and decide whether the situation is dangerous. If the reported situation is dangerous, the server will notify the rescue services immediately (step 3). In the fourth step, rescue services will help injured victims or secure the area.

Many types of IoT devices equipped with cameras can be used for this system. Also, we can employ users and their smartphones in it. The whole process of system operation should satisfy some security requirements. It should implement and realise the appropriate security protocol for communication between devices connected to the system (including the trusted server and the rescue services). The security protocol should guarantee high security in inter-entity communication, including scalability, authenticity, assault resistance, and data confidentiality. Ensuring that unauthorised parties cannot access the sent information is connected to data confidentiality. Ensuring data is not altered or lost while in transit entails maintaining data integrity. Verifying the identification of users or communication systems is referred to as authenticity. Attack resistance protects users and their data from various network threats. Scalability is the ability to securely communicate with many users or systems while accommodating the addition of new users or systems without requiring a complete protocol change. The protocol should also incorporate AAA (Authentication, Authorization, Accounting)

logic, whose elements govern user identification within the network, enforce user rules, and log session statistics (Steingartner et al., 2022).

Such a system involves risks, for example, associated with security, privacy, data storage, or AI use. Security and privacy risks are associated with many threats from computer networks. Each computer system is the target of cyberattacks. Hackers have many abilities and tools to break into the computer system, steal users' data and then use them in an unethical way. So the users can lose their privacy.

The risk of storing data on servers is essential to using artificial intelligence and information technologies. If the data stored on the servers contain personal information, there is a risk of unauthorised access or use by third parties. Cyberattacks, data leaks or inadequate security measures can violate users' privacy. Servers that store data are at risk of mentioned cyberattacks. Hackers may try to take control of servers or steal stored data for illegal use, such as identity theft or blackmail. Regardless of the cause (hardware failure, human error, attacks), there is a risk of losing server data. If proper backup and data redundancy strategies are not in place, a server failure can permanently lose valuable information. Storing data on servers requires proper management. Configuration errors, insufficient security measures or improper procedures can lead to unauthorised access, loss or accidental disclosure of data. Storing data on servers requires compliance with relevant laws and regulations, such as the General Data Protection Regulation (Voigt & Von Dem Bussche, 2017) in the European Union. Failure to comply with these requirements may lead to legal consequences, financial penalties and loss of user trust.

Using artificial intelligence (AI) in such systems carries certain risks. First, AI can make mistakes or produce unpredictable results. Learning algorithms may base their decisions on training data that may be incomplete, error-prone, or biased. This can lead to incorrect or unfair decisions. If systems are wholly dependent on AI, failures, programming errors, or technical issues can cause severe disruptions in the functioning of these systems. This can have negative consequences for society. AI can pose ethical and responsibility challenges. Decisions made by AI systems can have profound social impacts. We must be sure that AI's decision about dangerous situations is correct and will not cause human death.

To conclude, this on-going research is highlighted in this paper, where it discusses the architecture of the proposed system and its requirements, challenges and risk. This framework has considered many factors, such as previous research outcomes of the author, existing frameworks in this context, most importantly, the need and requirements for a safe, functional smart city. Given that there is lack or no such proposed framework, this is a significant contribution that can be used as a starting framework for other contexts.

KEYWORDS: Smart cities, AI, ambulance services, risk and security.

REFERENCES

Internet of Things. (2022). In Transactions on Computer Systems and Networks. Springer Nature. https://doi.org/10.1007/978-981-19-1585-7

Joshi, S., Saxena, S., & Godbole, T. (2016). Developing smart cities: An integrated framework. *Procedia Computer Science*, *93*, 902-909.

Steingartner, W., Možnik, D., & Galinec, D. (2022, November). Disinformation Campaigns and Resilience in Hybrid Threats Conceptual Model. In *2022 IEEE 16th International Scientific Conference on Informatics (Informatics)* (pp. 287-292). IEEE.

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

Tura, N., & Ojanen, V. (2022). Sustainability-oriented innovations in smart cities: A systematic review and emerging themes. *Cities*, 103716.

Voigt, P., & Von Dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). https://doi.org/10.1007/978-3-319-57959-7