

Enhancement of Public Safety using Internet of things Comprehensive Study

Manya Goel¹ and Juhi Singh²

¹⁻²Department of computer science and engineering Manipal University Jaipur, Jaipur, India
Email: goelmany0431@gmail.com, juhi.singh@mujaipur.edu

Abstract— This research paper critically examines the enhancement of public safety by the use of the Internet of Things (IoT). The Internet of Things (IoT) is an innovative technology with vast potential for improving public security and safety in many areas. We discussed the application of IoT in public safety, such as its application in smart cities, environmental monitoring, and crisis management. The research elaborates on the IoT system architecture, noting the five-layer architecture and its significance to security and privacy in public safety systems. We also provide case studies of actual application of IoT to public safety scenarios. The paper concludes by examining the potential of IoT in public safety and the necessity of robust security measures to thwart any vulnerabilities in IoT-based public safety systems.

Index Terms— IOT environment, Smart city, Sensors, Public Safety.

I. INTRODUCTION

A system of devices, actuators, and sensors that talk to one another so that data can be shared and passed over the Internet is the IoT. Devices can include a huge array of objects within our environment [1,2]. With Cisco suggesting that over 50 billion distinct gadgets would belong to the IoT by 2020 [3]. These systems provide an integrated framework with comprehensive functionality and responsive procedures, enhancing cities capacity to address public catastrophes. IoT applications in public safety regulation have enhanced regulatory technology and are anticipated to provide significant economic advantages. IoT integration in public sector services is projected to provide \$4.6 trillion in net profit worldwide over the next decade [4]. Use of IoT technology greatly improves public safety by virtue of several applications and systems. Use of IoT toward public safety has immense potential to improve the monitoring, response, and

management of safety issues in diverse contexts [5]. The devices used in the IoT context are designed to autonomously send data over the network, each possessing a unique identity [6]. The architecture of the Internet of Things often has many levels. The five-layered architecture is a prevalent concept that tackles security and privacy concerns associated with IoT-enabled services and applications [7]. A different viewpoint proposes a three-tiered system architecture [8]. The layers usually include an application layer for data transmission and a perceptual layer for data acquisition. Certain devices may have supplementary layers for improved functionality and security. While IoT presents tremendous prospects for the development of industrial applications, including smart grids, smart cities, and smart manufacturing, it concurrently creates substantial security issues [9,10] The rapid proliferation of linked devices has intensified security issues, making security and privacy a paramount problem for IoT.

Researchers are investigating many security strategies, including data analytics, to enhance security inside IoT ecosystems [11]. Urban living has become impossible Without IoT, which makes life more comfortable by supplying information that eventually raises standards of living. To effectively harness these advantages, it is essential for government officials and public safety organisations to study the whole potential of IoT while concurrently solving the accompanying security problems. The following sections of the research paper are organized as follows: A review of the literature is presented in section 2, the IoT system architecture is described in Section 3, and Section 4 provides case studies that illustrate real-life applications of IoT for public safety. Section 5 ends this analysis and proposes more avenues for research.

II. RELATED WORK

Interestingly, although IoT applications in public safety hold promise, challenges exist to be overcome. There are piecemeal cybersecurity solutions, an absence of end-to-end standards, and a relative dearth of well-developed and vertical applications. In addition, ensuring crowdsourced data is reliable for public safety applications is crucial, as evidenced by the Trustworthy Sensing for Crowd Management (TSCM) project, which can reduce the impact of malicious users by 75% [17]. In summary, the use of IoT in public safety covers various areas of application, ranging from food safety, disaster management, smart cities, and personal health monitoring. The combination of IoT with technologies like cloud computing, fog computing, and multi-access edge computing (MEC) could improve its performance in meeting the stringent requirements of public safety applications [18]. As the technology progresses, it will be crucial to overcome security issues and standardisation challenges to harness the full potential of IoT in public safety.

III. ARCHITECTURE OF IOT ENVIRONMENT

The infrastructure of an IoT setting pertaining to public safety is a combination of multiple technologies. These technologies assist in creating smart, effective, and secure systems. These architectures typically employ edge-fog-cloud computing, blockchain, and microservices to address scalability, security, and performance challenges. Integration of edge-fog-cloud paradigms enables unimpeded public safety services with improved processing power and low latency for response-hungry applications [19]. The multi-layered solution enables local data analysis at the edge, reducing the amount of sensitive data to be transferred to the cloud [20]. One of the central pillars of this is Blockchain-Enabled Decentralised Microservices Architecture (BlendMAS), which comprises a permissioned blockchain-based network and containerised microservices governed by smart contracts. This provides decentralised, scalable, and secure data handling and access control for distributed IoT based smart public safety systems. The BlendSPS system makes use of a hybrid block chain model and microservices-based security features to provide a decentralised security framework with the attributes of immutability, auditability, and traceability [21]. Microservices architecture is used to deliver scalable and adaptable services within dispersed IoT systems. The architecture enables the decoupling of security functions into separate containerised microservices, which may be run on edge and fog computing nodes. Microservices and blockchain integration enable a decentralised security mechanism defined by traceability, auditability, and immutability to enable secure data exchange and operations among participants [21]. The use of Software Defined Networks (SDN) to provide low-power wireless personal area network (6LowPAN) devices with on-demand and efficient network resources is the other necessary factor. IoT monitoring and control applications are complimented by this new architecture [28]. In addition, IoT based metropolitan public safety emergency management early warning systems can achieve all-round monitoring and control, authentic forecast and efficient response [12]. The use of edge-fog-cloud computing, blockchain, and microservices in IoT public safety infrastructures offers a unified solution to scalability, security, and performance issues in massive heterogeneous networks. The solution offers a decentralised, scalable, and secure environment for data sharing and access control in smart public safety systems [23].

IV. IOT BASED SYSTEM FOR PUBLIC SAFETY

IoT-based technologies have shown efficacy when integrated for public use. The convergence of IoT, Edge, and Fog Computing technologies may substantially improve public safety in smart cities by facilitating real-time monitoring, detection, and reaction to crises. These technologies provide a holistic solution to tackling significant issues in urban settings. The primary objectives of the ecosystem are Presented below is an IoT based ecosystem for public safety:

A. Key Objective

The key objective of the IOT based ecosystem which can be used for public safety are:

- Real-Time Threat Detection – Identify security threats, accidents, and disasters instantly
- Faster Emergency Response – Use AI and Edge processing for immediate action.
- Predictive Analytics – Prevent incidents using real-time monitoring and historical data.
- Decentralized Computing – Reduce latency using Edge and Fog computing.

B. System Architecture

The system architecture typically consists of four key layers:

- A device or perception layer for data collection from IoT sensors,
- An edge layer for real-time processing at the device level
- A fog layer for intermediate processing and local decision-making,
- A cloud layer for storage, analytics, and global control

This hierarchical structure enables efficient power management in IoT device communication and secure data management.

C. System Workflow

The intelligent crime detection and emergency response system combines IoT devices, edge computing, fog computing, and cloud infrastructure to establish a strong public protective system.

- It starts with threat identification using AI-powered CCTV cameras at the IoT and edge level to detect suspicious behaviour and categorize likely crimes [31].
- The initial identification is then verified by fog nodes, which cross-match information from several sensors to verify the incident before notifying the police
- Once an incident is established, the system is efficient in allocating resources. The closest police officers are deployed, and where human officers are not available, drones are used for rapid response.

The intelligent crime detection and emergency response system combines IoT devices, edge computing, fog computing, and cloud infrastructure to establish a strong public protective system.

- It starts with threat identification using AI-powered CCTV cameras at the IoT and edge level to detect suspicious behavior and categorize likely crimes [31].
- The initial identification is then verified by fog nodes, which crossmatch information from several sensors to verify the incident before notifying the police.
- Once an incident is established, the system is efficient in allocating resources. The closest police officers are deployed, and where human officers are not available, drones are used for rapid response.

The IoT framework utilizes hierarchical edge-fog-cloud deployment to distribute computing and intelligence and offer solutions to data volume, latency, and security attacks. Use of UAVs and secure communication protocols greatly enhances the quality and dependability of the system [27]. Technology enhances its crime prediction ability and provides urban planning by storing event data for long-term analysis to enable a proactive public safety strategy in smart cities.

IV. CASE STUDY

IoT technologies have various uses in public safety, offering new solutions for enhanced emergency response, disaster management, and overall safety in smart cities. Many case studies confirm the real-world application and usefulness of IoT in public safety.

A. Drone and IoPST

The collaboration between drones and the Internet of Public Safety Things (IoPST) has proven significant to enhance public safety and disaster management. This interoperability makes possible real-time analytics, monitoring, and advanced decision-making in intelligent cities [13]. Drones can be employed to offer rapid wireless communication services and extend surge capacity right after a disaster, reaching hard-to-reach areas and offering quick coverage and connectivity [13]. Drones have, for example, been utilized in a number of mission-critical scenarios to collect and transmit sensitive information to ground stations [19]. The use of AI and drones in the IoT network, for example, has revolutionized disaster management protocols in natural disasters. Drones have been employed for monitoring, surveillance, and data collection in affected areas, thus enhancing community resilience [22]. Medical delivery drones have also become a vital component of

sophisticated health care systems, leveraging 5G and IoT technology to offer a range of medical services in remote or remote locations [23].

B. FIESTA-IoT platform

FIESTA-IoT platform was used in the pilot trials in Gold Coast, Australia, and Santander, Spain, to facilitate crowd control applications in smart cities [24]. Crowd Mobility Analytics System and the Crowd Counting and Location System were two IoT systems that were used in the pilot trials, and both were included in the Smart, Santander testbed. [25]. Regular smart city applications and services, including crowd control, were facilitated by this infrastructure.

A real-time parking availability system was implemented in the city center by the city using open data sets and IoT technology in order to provide important information to tourists and citizens [26]. Though the factual information about the pilot on the Gold Coast is not available in the given context, it is probable that the same applications were probably executed there. The capability of the FIESTA-IoT platform to support a range of IoT applications for crowd management in smart cities implies that both sites witnessed the same scale of crowd travel analysis and real-time tracking. These pilot programs demonstrate the practical implementation of IoT technology in urban areas to enhance crowd management and urban services. Merging various sensors and data sources through platforms such as FIESTA-IoT allows cities to have valuable insights into people's movements and mobility patterns, thereby making urban management responsive and efficient.

C. IoT-based smart emergency response systems

IoT-enabled smart emergency response systems have been developed to enhance safety and effectiveness in a number of domains, including cars, homes, and smart campuses. One example of an effective application is the LPWAN-enabled emergency response system implemented at Hazara University in Pakistan for visually impaired individuals [29].

This system had 98% reliability in sending timely warnings and vital information to users with disabilities. The Smart Accident Precognition System (SAPS) integrated with Google Assistant, offers a new technique for vehicle safety in the car sector [30]. This technology monitors numerous aspects of the vehicle, such as speed, distance, and safety features, and stores real-time information on the cloud. The Google Assistant interface provides for remote operation of automobile functions and automated tasks, thus enhancing convenience and safety. These illustrations highlight the potential of IoT-based emergency response systems to promote safety and efficiency in most environments. Through implementation of technology such as LPWAN, cloud computing, and AI-powered assistants, these systems could offer timely warnings, streamline critical processes, and ensure better user experience. The effectiveness of the deployments demonstrates the feasibility and effectiveness of IoT-based solutions in preventing safety challenges and promoting emergency response competencies across different environments.

VI. CHALLENGES

IoT configurations utilized for public safety face various challenges regarding security, privacy, scalability, and technical implementation. Security and privacy are paramount in IoT deployments for public safety. The collection and sharing of sensitive data through networked devices challenge data confidentiality, integrity, and authenticity. There is risk of unauthorized access and data leakage. Potential misuse of personal information gathered by IoT sensors and appliances [32]. Enforcing tight security processes and data protection protocols is critical in upholding public trust and preventing vulnerabilities in critical infrastructure. Although IoT has significant potential for enhancing public safety, at the same time it also brings new risks and opportunities in cybersecurity.

The combination of edge computing and artificial intelligence with the Internet of Things holds promising research possibilities while at the same time bringing increased security issues. There is another paradox in the limited resources of IoT devices, which limit their ability to implement complex security protocols, yet they handle a large volume of sensitive information. New approaches are being explored to address these challenges. Blockchain technology is starting to be considered as an effective means for enhancing security and privacy for IoT devices. The use of distributed architecture and sophisticated encryption methods can ensure data integrity and access management. Additionally, the creation of smart city frameworks and standardized models can better facilitate efficient use of IoT in public safety applications. Overcoming these challenges requires collaboration among governments, industry players, and citizens to ensure proper and fair application of IoT technology for public safety.

VII. CONCLUSION

The IoT for public safety presents an excellent chance to enhance emergency response, criminal prevention, and community well-being. The IoT-based environment and architecture offer a strong platform to integrate heterogeneous sensors, devices, and data sources, improving the responsiveness and efficiency of the public safety ecosystem. Public safety IoT architecture typically comprises three major layers: the perception layer (data collecting devices and sensors), the network layer (transmission and data communication protocols), and the application layer (systems of decision-making and data analysis). The IoT architecture enables real-time gathering, distribution, and processing of data, which results in faster and more informed public safety response. The implementation of IoT in public safety poses challenges, particularly in security and privacy. The surge of IoT devices within critical infrastructure increases the level of risk from cyber-attacks and data breaches, therefore necessitating tight security measures. The massive amounts of data generated by IoT devices require efficient processing and analytical methods in order to obtain important insights. In order to confront future issues, several areas require increased research and development. These are: 1. Enhancing the robustness and security of IoT systems in public safety use cases, particularly against cyber attacks. 2. Advancing sophisticated data analysis technologies, such as AI and machine learning, for better prediction capabilities and informed decision-making in emergency situations. 3. Overcoming interoperability issues in order to facilitate seamless communication between different IoT devices and systems of various public safety organizations. 4. Examining the potential of edge computing and 5G technologies in offering accelerated, localized

REFERENCES

- [1] Nawir, M., Lynn, O. B., Amir, A., & Yaakob, N. (2016). Internet of Things (IoT): Taxonomy of security attacks. 321–326. <https://doi.org/10.1109/iced.2016.7804660>
- [2] Kamble, A., & Bhutad, S. (2018). Survey on Internet of Things (IoT) security issues & solutions. 307–312. <https://doi.org/10.1109/icisc.2018.8399084>
- [3] Ma, Y., Wu, C., Chen, H., Jiang, C., & Ping, K. (2018). Internet of Things applications in public safety management: a survey. *Library Hi Tech*, 38(1), 133–144. <https://doi.org/10.1108/lht-12-2017-027>
- [4] Du, C., & Zhu, S. (2012). Research on Urban Public Safety Emergency Management Early Warning System based on Technologies for the Internet of Things. *Procedia Engineering*, 45, 748–754. <https://doi.org/10.1016/j.proeng.2012.08.234>
- [5] Joel, M. R., Manikandan, G., & Bhuvaneswari, G. (2023). An Analysis of Security Challenges in Internet of Things (IoT) based Smart Homes. 57, 490–497. <https://doi.org/10.1109/icears56392.2023.10085106>
- [6] Alansari, Z., Soomro, S., Alshaer, J., Anuar, N. B., Miraz, M. H., Kamsin, A., & Belgaum, M. R. (2018). Internet of Things: Infrastructure, Architecture, Security and Privacy. 10, 150–155. <https://doi.org/10.1109/icecome.2018.8658516>
- [7] Zhao, K., & Ge, L. (2013). A Survey on the Internet of Things Security. 663–667. <https://doi.org/10.1109/cis.2013.145>
- [8] Abosata, N., Emmanouilidis, C., Inalhan, G., & Al-Rubaye, S. (2021). Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors (Basel, Switzerland)*, 21(11), 3654. <https://doi.org/10.3390/s21113654>
- [9] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: https://doi.org/10.1080/19393555.2018.1458258 A Global Perspective*, 27(3), 162–182.
- [10] Adewuyi, A., Oloke, K., Abijo, I., Tsambatare, T., Enyiorji, P., Oladele, A., & Ajayi, O. (2024). The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. *World Journal of Advanced* <https://doi.org/10.30574/wjarr.2024.23.1.1993> Research and Reviews, 23(1), 379–394.
- [11] Soni, T., Uppal, M., & Gupta, D. (2023). Bibliometric Analysis on Security of Different Layers in Internet of Things (IoT) Environment. 1–6. <https://doi.org/10.1109/esci56872.2023.10099986>
- [12] Abass, T., Bature, J., Eruaga, M., & Itua, E. (2024). ADVANCING FOOD SAFETY THROUGH IOT: REAL-TIME MONITORING AND CONTROL SYSTEMS. *International Medical Science Research Journal*, 4(3), 276–283. <https://doi.org/10.51594/imsrj.v4i3.919>
- [13] Alsamhi, S., Gupta, S., Ma, O., & Ansari, M. (2019). Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. *Drones*, 3(1), 13. <https://doi.org/10.3390/drones3010013>
- [14] Rauniyar, A., Feng, B., Thanh, D. V., & Engelstad, P. (2016). Crowdsourcing-Based Disaster Management Using Fog Computing in Internet of Things Paradigm. 17, 490–494. <https://doi.org/10.1109/cic.2016.074>
- [15] Minoli, D., Occhiogrosso, B., & Sohraby, K. (2017). IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems. *IEEE Internet of Things Journal*, 4(1), 269–283. <https://doi.org/10.1109/jiot.2017.2647881>
- [16] Kantarci, B., & Mouftah, H. T. (2014). Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things. *IEEE Internet of Things Journal*, 1(4), 360–368. <https://doi.org/10.1109/jiot.2014.2337886>

- [17] Zanzi, L., Giust, F., Sciancalepore, V., Cirillo, F., Klas, G., Costa-Perez, X., & Mangiante, S. (2019). Evolving Multi-Access Edge Computing to Support Enhanced IoT Deployments. *IEEE Communications Standards Magazine*, 3(2), 26–34. <https://doi.org/10.1109/mcomstd.2019.1800009>
- [18] Alsamhi, S., Gupta, S., Ansari, M., & Ma, O. (2019). Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. *Drones*, 3(1), 13. <https://doi.org/10.3390/drones3010013>
- [19] Tanveer, M., El-Latif, A. A. A., Ahmad, M., Nguyen, T. N., & Khan, A. U. (2023). Towards a Secure and Computational Framework for Internet of Drones Enabled Aerial Computing. *IEEE Transactions on Network Science and Engineering*, 10(5), 3058–3070. <https://doi.org/10.1109/tnse.2022.3151843>
- [20] Kuchuk, H., & Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: a review. *Advanced Information Systems*, 8(2), 65–78.
- [21] Xu, R., Nikouei, S. Y., Chen, Y., Blasch, E., & Aved, A. (2019, July). Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 564–571). IEEE.
- [22] Singh, R., Manoharan, G., & Singh, S. (2024). Strategic Deployment of AI and Drones Enhancing Disaster Management in Natural Disasters (pp. 172–203). *igi global*. <https://doi.org/10.4018/979-8-3693-3896-4.ch009>
- [23] Ray, P. P., & Nguyen, K. (2020, August 9). A Review on Blockchain for Medical Delivery Drones in 5G-IoT Era: Progress and Challenges. <https://doi.org/10.1109/icccworkshops49972.2020.9209931>
- [24] Solmaz, G., Munoz, L., Kovacs, E., Sanchez, L., Santana, J. R., Wu, F.-J., Sotres, P., & Cirillo, F. (2019). Toward Understanding Crowd Mobility in Smart Cities through the Internet of Things. *IEEE Communications Magazine*, 57(4), 40–46. <https://doi.org/10.1109/mcom.2019.1800611>
- [25] Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E., & Pfisterer, D. (2013). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks*, 61, 217–238. <https://doi.org/10.1016/j.bjp.2013.12.020>
- [26] Lanza, J., Gutiérrez, V., Sánchez, L., Muñoz, L., Galache, J., Sotres, P., & Santana, J. (2016). Smart City Services over a Future Internet Platform Based on Internet of Things and Cloud: The Smart Parking Case. *Energies*, 9(9), 719. <https://doi.org/10.3390/en9090719>
- [27] Grover, I. (2025). Fog Computing and AI for Real-time Disaster Response in Smart Cities. *Risk Assessment and Management Decisions*, 2(2), 70–79.
- [28] Miguel, M. L., Jamhour, E., Pellenz, M. E., & Penna, M. C. (2018). SDN architecture for 6LoWPAN wireless sensor networks. *Sensors*, 18(11), 3738.
- [29] Safi, H., Algarni, A., Jehangiri, A. I., Ala'Anzy, M. A., Ahmad, Z., & Alramli, O. I. (2024). Design and Evaluation of a Low-Power Wide-Area Network (LPWAN)-Based Emergency Response System for Individuals with Special Needs in Smart Buildings. *Sensors (Basel, Switzerland)*, 24(11), 3433. <https://doi.org/10.3390/s24113433>
- [30] Menon, V. G., Jacob, S., Joseph, S., Sehdev, P., Khosravi, M. R., & Al-Turjman, F. (2020). An IoT enabled intelligent automobile system for smart cities. *Internet of Things*, 18, 100213. <https://doi.org/10.1016/j.iot.2020.100213>
- [31] Aldowah, H., Umar, I., & Ul Rehman, S. (2018). Security in Internet of Things: Issues, Challenges and Solutions (pp. 396–405). *springer*. https://doi.org/10.1007/978-3-319-99007-1_38
- [32] V. Malik and S. Singh, “Security risk management in IoT environment,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 697–709, May 2019, doi: 10.1080/09720529.2019.1642628.