RESEARCH PAPER
Future Research in AI & IoT, 2025, 1(2)
Homepage: https://frai.journals.umz.ac.ir/
DOI:

Improving security and privacy in an IoT based smart city application using Blockchain

Reyhane Parandoush[1], Shahriar Bijani[2]*

[1] *Applied Research Lab, Department of Computer Science, Shahed University, Tehran, Iran, r_parandoush@yahoo.com*

[2] *Applied Research Lab, Department of Computer Science, Shahed University, Tehran, Iran, bijani@shahed.ac.ir*

Article Info
Received -----
Accepted -----
Available online -----

Keywords:
Third-Generation Blockchain Technology;
Information Security;
Agent-based System;
Crisis Management.

Abstract:
Effective crisis management is, in most cases, fundamentally reliant on human activity and interpersonal communication. Establishing communication among various groups through intelligent and reliable interactions significantly enhances crisis management capabilities. To this end, the present study proposes an agent-based system designed to facilitate communication among stakeholders and enable fact-based decision-making by emergency response agents. Furthermore, the system leverages the new generation of blockchain technology as a secure and trustworthy platform for communication between emergency agents and citizens. The integration of blockchain technology introduces innovative methods for generating and transferring relevant data, thereby supporting optimal decision-making in crisis response scenarios. This study designs and analyzes a distributed crisis management system based on intelligent agents, deployable within the Internet of Things (IoT) infrastructure, and built upon third-generation blockchain technology. The primary objective of this system is to ensure secure and trustworthy information sharing among citizens, thereby enabling emergency responders to make informed decisions grounded in the accuracy of citizen-reported data.

***Corresponding Author:** bijani@shahed.ac.ir

Supplementary information: Supplementary information for this article is available at https:// frai.journals.umz.ac.ir/
Please cite this paper as:

1. Introduction

A crisis may be defined as a state of abnormality that arises from natural instability or human actions within various domains. Such an event typically generates unexpected and adverse consequences for a particular segment of society. To ensure that crisis management efforts are effectively orchestrated and integrated, information exchange among rescue teams must be facilitated. Indeed, the utilization of diverse information by rescuers enhances their ability to make optimal decisions and collaborate more efficiently in addressing crisis. Existing data management systems utilized for crisis management often fall short in their capacity to adapt to diverse scenarios. Moreover, the complexities and unpredictability of crisis make a centralized command center inadequate to address the challenges that emerge. Therefore, it is essential to empower distinct teams of rescuers to independently address the exigencies that arise at a local level. In order to facilitate effective information exchange between these field-based rescuers, it is crucial to adopt appropriate methods and techniques that can enhance the sharing of critical information. The design of an effective information flow system for crisis management necessitates careful consideration of several fundamental factors. Notably, the compatibility and flexibility of information, real-time information transfer, and security and accuracy of the shared data represent critical issues that must be thoroughly evaluated. Only by addressing these factors can an information flow system be designed that effectively supports field-based rescuers in addressing the challenges that emerge during crisis situations.

Currently, intelligent agents are extensively employed across a broad range of operational and research contexts. These agents' intelligence is embedded within the software and is activated through a lightweight program. The awareness of an agent within a system is proportional to the

ISSN

extent of information that the agent has access to. In situations where information exchange occurs between agents, it is imperative to implement a mechanism that can effectively verify the accuracy and reliability of the received data. The objective of this paper is to introduce an intelligent agent-based framework that leverages third-generation Blockchain technology for crisis management purposes. By utilizing this framework, critical information can be securely and efficiently exchanged among agents, thereby enhancing the overall effectiveness of crisis management efforts.

The proposed framework is intended to facilitate the secure and dependable exchange of information between citizens and rescuers. This enables rescuers to obtain insights into the accuracy of citizen reports, thereby enhancing their ability to make informed decisions related to crisis management. However, a critical question arises concerning how to ensure the accuracy of data transmitted by citizens to the rescue team. The paper is structured as follows. Section 2 offers a detailed overview of blockchain technology, with a specific focus on the advancements and distinctive features of third-generation blockchain. Section 3 reviews the existing literature on the use of software agents and blockchain technology as effective tools for enhancing disaster response capabilities. Section 4 details the process of designing a third-generation Blockchain technology system that leverages software agents. Finally, Section 5 outlines potential directions for future research.

2. Background

Blockchain is a decentralized network and distributed database structure that serves as a public repository for immutable, non-expiring, and non-modifiable data. Among its most notable features are transparency and interoperability. Interoperability enables organizations to coordinate resources using Blockchains without the need for central management or human intervention. Additionally, the transparency of the Blockchain ensures that records are accessible and unalterable for each network member. As a result, the Blockchain is a reliable technology for organizing communication and facilitating secure data transfer. In recent times, entrepreneurs across diverse industries have become increasingly acquainted with Blockchain technology and its potential applications. One of the most popular use cases for Blockchain is to track financial records, as exemplified by the introduction of Bitcoin in the white paper titled "Bitcoin - A Peer-to-Peer Electronic Cash System". It is worth noting that besides Bitcoin, there are other cryptocurrencies that leverage Blockchain technology. For instance, IOTA is a third-generation Blockchain technology that employs the Tangle graph. Unlike Bitcoin, IOTA does not require the approval of the majority of network members to record transactions, thus resolving the scalability problem inherent in Bitcoin. Tangle refers to a distributed ledger technology specifically designed for the Internet of Things (IoT). In Tangle, the data of each transaction is stored in the structure of a directional acyclic graph (DAG), where each node in the graph represents a transaction. It is worth noting that the term "acyclic" implies that no node in the graph can refer to itself, as shown in Figure 1. DAG is particularly well-suited for applications that require high scalability, capable of processing thousands of transactions per second. IOTA, which is built on Tangle, provides a public interface for IoT and enables fast connectivity between different devices. The IOTA framework also facilitates micro-payments between humans and devices. In the IOTA network, every user has the ability to both create and validate transactions in a concurrent manner. To initiate a new transaction, an individual must engage in the network's consensus process by selecting two unconfirmed transactions on the network using a tip selection algorithm and validating them. These selected transactions are then propagated as quickly as possible throughout the network. In order to prevent spam and potential Sybil attacks (When an attacker attempts to subvert the network by creating multiple identities), a small-scale proof of work is required to be completed with each transaction. This involves a minimal amount of computational work. In the IOTA network, the validation of a transaction involves multiple steps, including checking the transaction signature, proof of work, and ensuring its consistency with previous transactions, both direct and indirect. The transaction rate, represented by the parameter λ, is kept constant on the network. If this value is considered too small, any new transaction can only be connected to the previous transaction, leading to a potential bottleneck in the network's scalability (Figure 2). Conversely, if the incoming transaction rate is too high, only the primary transaction is available to connect the new transactions to the network, which may result in a less reliable and secure system.

To mitigate these issues, IOTA employed a centralized node, called a coordinator, which serves as an auxiliary network assistant in the early stages of IOTA's development. All transactions were first processed through the coordinator, which validated the transactions and added them to the Tangle. In IOTA 2.0, the coordinator has been removed. The objective of the present investigation is to evaluate the potential application of Tangle technology to enhance the accuracy of reports filed by citizens. Specifically, the proposed approach involves conducting background checks on reporting individuals and leveraging the results to establish a credibility score that reflects their reliability in providing truthful and accurate information. Subsequently, this score is conveyed to the relevant rescue teams in a separate message, thus enabling them to prioritize their response efforts accordingly.

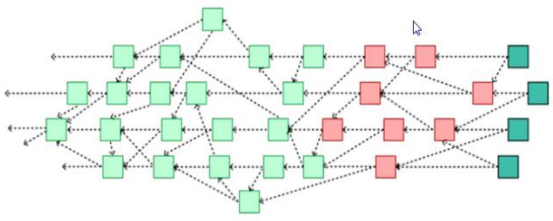

Figure 1. DAG graph in IOTA.

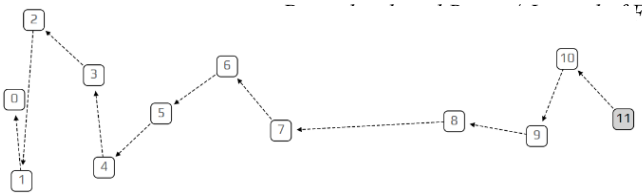

Figure 2. The average transaction rate (λ) is too small.

3. Related works

Alhavan et al. [1] propose the CoviReader architecture, a decentralized data management framework built on IOTA's Tangle infrastructure for controlling the COVID-19 pandemic in smart cities. The architecture is designed to store and verify individuals' health status data in a tamper-proof and privacy-preserving manner. The solution includes two operational modes: a Transaction Plan for real-time registration and inquiries, and a Big Data Plan for crisis management and data analytics. By leveraging Tangle's distributed and scalable features, the authors aim to ensure data integrity and anonymity while facilitating fast access and decision-making for health authorities. While the system promises strong protection against data manipulation, a key limitation lies in the lack of semantic-level conflict detection within the Tangle structure. If a malicious user issues two structurally valid but semantically conflicting health status transactions (e.g., "infected" vs. "healthy"), the architecture does not include a built-in mechanism to automatically detect or resolve such contradictions at the content level. The system relies on external mechanisms or post-facto aggregation for validation, which may be too late for critical, real-time applications such as access control or quarantine enforcement. This limitation weakens the architecture's ability to autonomously enforce trust in decentralized, adversarial environments.

Zhao et al. [2] present a decentralized cyber-physical system designed to promote adherence to public health protocols, specifically mask-wearing in confined environments such as aircraft cabins. The proposed solution leverages the IOTA Tangle, a directed acyclic graph (DAG)-based distributed ledger technology, in conjunction with a smart wearable device capable of detecting user compliance via environmental sensors (e.g., eCO_2 and TVOC). Compliance data is recorded pseudonymously on the Tangle using lightweight protocols (MAM, MQTT), ensuring both data integrity and user privacy. A central feature of the system is a feedback-based control algorithm whereby users deposit digital tokens as a form of economic stake. Token refunds are modulated based on individual and collective compliance levels, thus aligning user incentives with public safety objectives. The authors validate their approach through agent-based simulations and hardware-in-the-loop prototyping, demonstrating feasibility in both simulated epidemics and real-time environmental monitoring. The work is notable for integrating real-time behavioural sensing with distributed, tamper-resistant record-keeping, offering a privacy-preserving alternative to conventional enforcement mechanisms. However, limitations include reliance on heuristic sensor thresholds, limited generalizability of the simulation framework, and practical deployment challenges related to device adoption and digital infrastructure. This study contributes to the broader discourse on using distributed ledger technologies for real-world behavioural regulation and highlights the potential of DAG-based architectures for trustless, incentive-compatible governance mechanisms in public health contexts.

Also, [3] introduces Phonendo, a modular and event-driven platform designed to manage and securely publish data streams from wearable devices on distributed ledger technology infrastructures (DLTIs), specifically leveraging the IOTA Tangle. The authors address prevailing concerns in mobile health (mHealth), such as data tampering, privacy, and system scalability, by integrating wearable IoT data streams with a DAG-based, feeless, and permissionless ledger. Phonendo's architecture includes five key microservices—Reader, Manager, Storage, Verifier, and Publisher—each responsible for distinct stages of the data lifecycle, from device pairing and data capture to cryptographic verification and public storage on the IOTA network. The platform emphasizes data integrity, traceability, and privacy, supporting lightweight devices with limited computational capacity and ensuring modularity for diverse medical scenarios.

The authors justify their selection of IOTA over blockchain alternatives (e.g., Ethereum, Hyperledger Fabric) based on its fee-free nature, high throughput, and suitability for recurrent, low-volume data. They also explore practical applications such as health data certification, incentivization of healthy behaviours, and real-time condition tracking, while critically acknowledging limitations, including potential attack vectors, user misbehaviour incentives, and privacy risks from permanent data storage. Phonendo contributes to the growing body of research on secure, decentralized mHealth systems, offering a practical and extensible framework for real-world IoT-healthcare integration. The platform's open-source availability and support for future enhancements, including smart contracts and self-sovereign identity (SSI), further strengthen its relevance for researchers and developers in the domain.

4. Method

The use of multi-agent systems enables the simulation of rescue operations and enhances the efficiency of teams deployed at the scene of an incident. Agent-based modelling, as a novel approach to crisis management, offers distinct advantages over traditional modelling techniques. Specifically, it facilitates a deeper understanding of individual behaviours and needs in post-crisis contexts. This modelling framework also allows researchers to implement and evaluate diverse scenarios, including the distribution of aid and resources, cost monitoring, and logistical planning, thereby contributing to more effective and adaptive crisis response strategies. The integration of blockchain technology facilitates the development of novel methods for generating, transmitting, and accessing crisis-related data,

thereby enabling more effective and informed decision-making in crisis management. The objective of this study is to design an agent-based system leveraging third-generation blockchain technology to support decision-making and management in crisis situations.

4.1. Agent-based system design

Gent-based modelling represents a contemporary approach to the development of crisis response systems. The system's operational requirements are detailed in Figure 3. Citizens can interact with the system either to request assistance or to report an incident. The reporting individual is expected to specify the type of crisis, its geographical location, and, if possible, provide an initial estimate of its severity. Upon receiving and analysing the submitted report, rescue teams assess the situation and determine an appropriate response strategy. This may involve initiating a direct response or, alternatively, forwarding the report to other rescue units within the network, thereby requesting additional support or delegating the crisis management responsibilities to a more suitable party. As illustrated in Figure 4, the system comprises two primary types of entities: information agents and rescue agents. The primary role of a rescue agent is to deliver professional assistance to individuals affected by the incident. However, citizens may also act as non-specialist rescuers by taking supportive actions to aid impacted individuals or mitigate the situation. A citizen who reports an incident is classified as an unknown and unverified information agent. In contrast, a rescuer or a senior-level authority submitting a report is regarded as a verified and trusted information agent. Additionally, sensor-based sources are also categorized as valid agents, given their predefined and authenticated operational parameters.

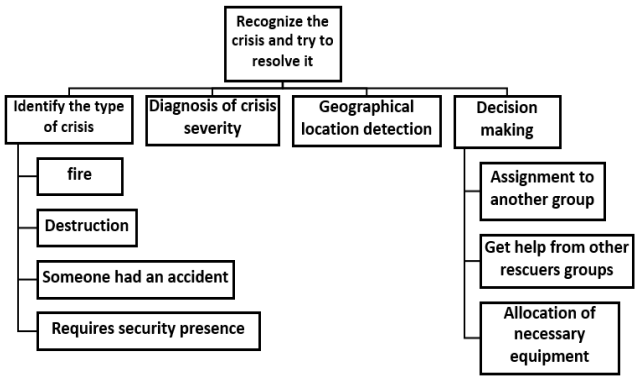

Figure 3. The operational requirements of the system.

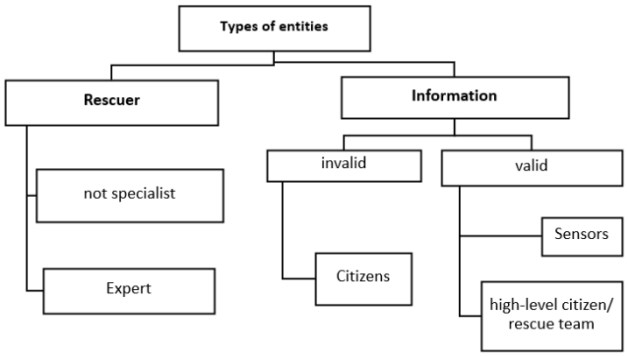

Figure 4. Type of entity.

The architecture of the agents is depicted in Figure 5. Each agent—whether an information agent or a rescue agent—includes communication layers responsible for interfacing with both the user and external components. The primary function of a specialist rescue agent is to deliver professional medical or logistical assistance to affected individuals. Additionally, it can transmit incident reports to other rescue teams. In contrast, the control layer of an information agent manages user interaction; if needed, it prompts the user to provide supplementary information. The collected data is then structured into a predefined format and submitted as a formal report. As previously stated, the core responsibility of an information agent is to report events; however, under certain conditions, it may also act as a non-specialist rescuer.

The following section aims to enhance a portion of the system's functionality by transitioning to a third-generation blockchain architecture. The primary objective of this upgrade is to enable secure and trustworthy data sharing among information agents. This design allows rescue agents to rely on the authenticity of incoming reports, thereby facilitating informed and timely decision-making in crisis situations with minimal reliance on human oversight or centralized control.

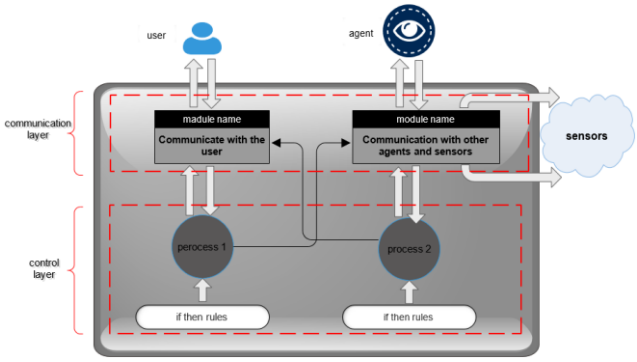

Figure 5. The architecture of the agents.

4.2. Third Generation Blockchain-based System Design

The system proposed in the previous section is designed to be applicable across a range of use cases. For the sake of clarity and simplicity, we assume that the reported incident pertains to a fire. In the conventional response process, the validity of such reports is typically verified by two appointed psychologists. However, if human validation is removed from the workflow, the responsibility for verifying the accuracy of citizen-submitted reports must be assumed by the rescue agent itself. Figure 6 illustrates the key factors a firefighter must consider to verify the authenticity of a received message. A high number of incident reports received by rescue agents may indicate an increased likelihood of a fire event.

The historical behaviour of the reporting agent represents another important factor in assessing report credibility. To facilitate this, a local database should be embedded within the rescue agent system, allowing access to the reporter's past activity. By consulting this record, the rescue agent can evaluate the reporter's reliability based on the frequency of previously submitted and verified reports. The integration of location services within rescue agents is also a valuable consideration. This functionality enables the rescue agent to determine the geographic position of the reporting entity and compare it with the location specified in the incident report. A significant discrepancy between these two coordinates may indicate that the reporter is not a verifiable or trustworthy source. Rescue agents may also assess the accuracy and reliability of incident reports by cross-referencing them with urban imagery corresponding to the reported location. For example, if an individual reports a fire in a commercial building at a specific geographic location, but available urban images do not indicate the presence of such a structure, the validity of the report may be called into question. This comparative analysis serves as an additional layer of verification to support informed decision-making. Sensors deployed across various locations can also generate incident reports and transmit them to the rescue agents. These sensor-based reports are considered alongside those submitted by other information agents, contributing to a more comprehensive situational assessment. Furthermore, the role of the reporting agent and the criticality of the reported location should be considered as distinct factors in the evaluation process. For instance, if a rescue agent acts as an information agent and issues a report regarding a fire, the receiving party should regard the report as inherently credible due to the agent's authoritative role. Conversely, if a report indicates a fire at a high-risk location—such as a gas station—immediate response should be prioritized, irrespective of the reporter's identity, due to the potential severity of the threat.

Figure 6. Items need to be investigated to determine the accuracy of a report.

In the proposed system, each information agent submits its report of an incident as a discrete transaction within the graph. Figure 7 illustrates how rescue and information agents work. Considering the inherent efficiency of the Tangle structure in achieving rapid transaction confirmations, it is reasonable to anticipate that incident report transactions will also be validated in a timely and reliable manner.

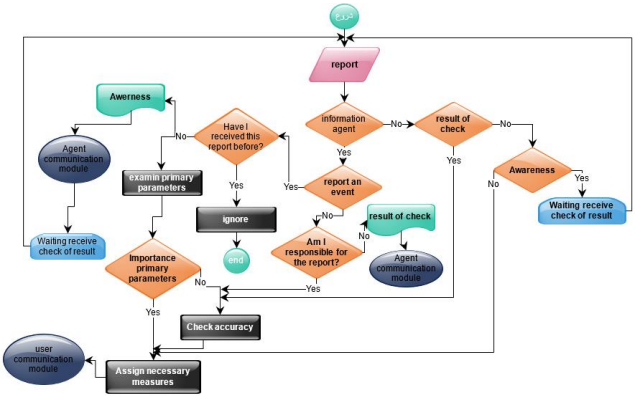

Figure 7. Operational mechanism of rescue agents.

5.Discussion and Conclusions

This study addresses the enhancement of security in crisis management by proposing the integration of Tangle technology within an agent-based system. Through this approach, rescue agents can verify the authenticity of incident reports, thereby supporting more reliable and informed decision-making during emergency response operations. In addition, agents can exchange information with one another to enhance the reliability of knowledge acquired for effective crisis response. This collaborative mechanism contributes to the development of a third-generation blockchain-based system. The proposed design overlooks the participation challenges faced by two categories of agents:

1. Those that do not provide any information about the reporter, and
2. Those that inadvertently acquire inaccurate data by connecting to invalid transactions.

As a result, additional mechanisms are required to address these shortcomings and ensure the integrity and reliability of agent interactions within the network. The distribution mechanism of transactions within the Tangle architecture has not been comprehensively explored in recent studies. Consequently, this topic presents a promising direction for future research.

6. Author Contributions

Conceptualization: Both authors designed the study.

Methodology: Ms. Parandoush developed the methodology and performed the experiments.

Analysis: Both authors analyzed the data and interpreted the results.

Original Draft Preparation: Ms. Parandoush wrote the initial draft of the manuscript.

Review and Editing: Both authors contributed to the review and editing of the manuscript.

Supervision: Mr Bijani supervised the project.

Both authors have read and approved the final version of the manuscript.

7. Acknowledgement

To improve the language and enhance clarity, writing software, such as Grammarly, was employed in the process of manuscript preparation.

References

[1] Alhavan, M., Azimi, A., & Manuel Corchado, J. (2022). A CoviReader Architecture Based on IOTA Tangle for Outbreak Control in Smart Cities during COVID-19 Pandemic. Medical Journal of the Islamic Republic of Iran. https://doi.org/10.47176/mjiri.36.180.

[2] Zhao, L., Ferraro, P., & Shorten, R. (2024). A smart mask to enforce social contracts based on IOTA Tangle. PLOS ONE, 19(3),e0292850. https://doi.org/10.1371/journal.pone.0292850.

[3] Moya, F., Miguel, F. J., Martínez, L., & Fco Javier Estrella. (2023). Phonendo: a platform for publishing wearable data on distributed ledger technologies. Wireless Networks. https://doi.org/10.1007/s11276-023-03458-7.

[4] D. Lombroso, M. Davison, and M. Wotton, "Development of an agent-based model to improve emergency planning in response to floods and dam failures," J. Hydroinformatics, vol. 25, no. 5, pp. 1610–1628, Sep. 2023.

[5] S. Mukherjee, I. Ray, I. Ray, H. Shirazi, T. Ang, and M. J. Kahn, "Attribute-Based Access Control for Healthcare Resources," in Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control (ABAC '17), Mar. 2017, pp. 29–40

[6] T.Cherniavska and B. Cherniavskyi, "Architecture-Oriented Agent-Based Model (AOAM) for Optimizing Transport Evacuation Management and Emergency Medical Assistance in the Context of the War in Ukraine: Challenges and Prospects," in Proceedings of the 3rd International Workshop on Information Technologies and Innovations (WITI 2024), CEUR-WS, vol. 3892, pp. 211–222, Nov. 2024

[7] C. Chen, C. Cole, H. Wang, and M. K. Lindell, "An interdisciplinary agent-based evacuation model: integrating the natural environment, built environment, and social system for community preparedness and resilience," Nat. Hazards Earth Syst. Sci., vol. 23, no. 3, pp. 733–750, Mar. 2023

[8] NIST, "Manufacturing Supply Chain Traceability Using Blockchain Related Technologies," National Cybersecurity Center of Excellence (NCCoE), Gaithersburg, MD, USA, NIST Project Brief, 2024.

[9] M. Rinaldi, M. Caterino, S. Riemma, R. Macchiaroli, and M. Fera, "Emergency Supply Chain Resilience Enhanced Through Blockchain and Digital Twin Technology," Logistics, vol. 9, no. 1, p. 43, Jan. 2025.

[10] L. McLaughlin, "Exploring the Use of Modern Supply Chain Techniques in Managing Natural Disaster Relief in the United States," Undergraduate Honors Theses, University of Pennsylvania, Philadelphia, PA, USA, Mar. 2024