Original Article
http://mjiri.iums.ac.ir
Medical Journal of the Islamic Republic of Iran (MJIRI)

Med J Islam Repub Iran. 2022 (28 Dec);36.180. https://doi.org/10.47176/mjiri.36.180

A CoviReader Architecture Based on IOTA Tangle for Outbreak Control in Smart Cities during COVID-19 Pandemic

Maryam Alhavan[1], Ali Azimi[1]*, Juan Manuel Corchado[2]

Received: 3 Oct 2022 Published: 28 Dec 2022

Abstract

Background: Reportedly, many of the data collected for detecting infected people are being used for other than healthcare purposes. On the other hand, fabricated digital COVID-19 test results will pose a danger to vulnerable people and to public health. This paper presents a CoviReader architecture designed for a smart city health information management system to manage outbreak of COVID-19 pandemic while protecting citizens' privacy and tamper-proofing their health status data.

Methods: We used IOTA as an infrastructure for data management. We introduced two plans: "Transaction Plan", handling daily interactions of citizens in a smart city and "Big Data Plan", providing the COVID-19 crisis headquarters with the aggregated data for curbing the pandemic.

Results: Through the proposed CoviReader architecture people's using IOTA tangle, people's health status data are readily available to the crisis headquarters and verification of the validity of the final file against data manipulation will also be possible by comparing the hash of the consolidated received file with the original hash of the file registered in the IOTA Tangle. Reported plans were capable of handling tamper proofed data delivery.

Conclusion: The proposed CoviReader architecture ensures the availability and at the same time constrains manipulation of data. The provided solution aids healthcare providers to control pandemic and at the same time to preserve commuting people's data for any unintended or illegal identity disclosure.

Keywords: COVID-19, Pandemic, Blockchain, Data Manipulation, Smart City, Identity Disclosure

Conflicts of Interest: *None declared*
Funding: *None*

This work has been published under CC BY-NC-SA 1.0 license.
Copyright© Iran University of Medical Sciences

Cite this article as: Alhavan M, Azimi A, Corchado JM. A CoviReader Architecture Based on IOTA Tangle for Outbreak Control in Smart Cities during COVID-19 Pandemic. *Med J Islam Repub Iran.* 2022 (28 Dec);36:180. https://doi.org/10.47176/mjiri.36.180

Introduction

According to the World Health Organization (WHO), the new coronavirus known as Coronavirus Disease 2019 (COVID-19) has been the source of the epidemic of Severe Acute Respiratory Syndrome-SARS and then Middle East Respiratory Syndrome –MERS (1). The first human cases of COVID-19 were reported officially in Wuhan City, China's Hubei Province, on December 2019 and the WHO classified the outbreak a "pandemic" in March 2020 (2). As of January 2023, more than 676,000,000 people have contracted the disease, of which more than 6.7 million died (3).

Due to the airborne nature, COVID-19 is severely spreadable in the society (4) and thus, acquiring people's health status information and data of infected citizens would be extremely helpful for authorities to limit and control the spread of the virus. However, according to the codes of ethics (5), patients' identities must be kept confidential, and exposing personal information without their consent or using them in other situations must be prohibited. This means citizens' rights to privacy outweighs the necessity and urgency of pandemic control and quarantine rules. Of the patients' rights to privacy is confidentiality of disease records. From psychological perspectives, people diagnosed with COVID-19 or newer variances may be shamed for their diagnosis. The self-conscious emotions

Corresponding author: *Dr Ali Azimi, azimia@khu.ac.ir*

1. Knowledge & Information Studies Department, Kharazmi University, Tehran, Iran
2. Computing and Control Department, University of Salamanca, Salamanca, Spain

↑What is "already known" in this topic:
People's health status should be controlled while commuting during pandemics.

→What this article adds:
A unique solution based on an IOTA Tangle was proposed to read the people's health status for COVID-19 infections and safeguard their identity against illegal disclosures.

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

such as shame and guilt can become a serious threat for mental health and as demonstrated in previous epidemics (HIV, Hepatitis B, Ebola) may affect mental well-being (6). Furthermore, codes of ethics enforce the healthcare agents to keep patients' records confidential even in the pandemic unless there is a serious risk of life for other people. Subsequently, the privacy violations and information disclosure may lead to a significant loss of public trust and a huge decrease in citizen's participation in information sharing.

In many countries, having a recent negative COVID-19 test is a golden admission for travelers' trip or citizens' commuting (7) during pandemic. Consequently, this golden ticket has motivated tampering COVID-19 test results by passengers or even residents. As a case of COVID-19 test fraud, the FBI has warned against manipulating the results of COVID-19 test by employees seeking to benefit from the pandemic (8). These are cases of data tampering efforts against quarantine regulations. Some governments have also been accused of misusing COVID-19 data privacy with unrestrained access to patients' COVID-19 information under the pretext of tracking the prevalence. For example, as stated in (9), the Singaporean government has admitted the tracing program data has been also available for the police. These violations reiterate the importance of using a tamper-proof infrastructure with an obligation of preventing invasion of privacy by governments.

During prevalence of highly contagious diseases, protecting information from unauthorized access is an essential demand to gain public trust and inspire people to share private information and tracing data. With the rise of smart cities, the healthcare ecosystem is increasingly benefiting from Internet of Things (IoT), 5G, AI, and other related advances in treatment and managing diseases. Also, access to advanced communication technologies such as virtual systems and remote applications offers new services in the field of healthcare (10-12). In parallel, the IoT is growing more mature, and the number of Internet-connected objects have been increased exponentially in the last five years. According to estimations provided by (3), the number of Internet-connected objects is estimated to reach to 30.9 billion by 2025. That number was about 3.8 billion in 2015. The success of using the IoT in smart cities (13) to tackle epidemics (14) and the vision of IoT, even in the short term, all say it will become an undeniable part of everyday life. Sareen et al (15), showed that integration of Internet of Medical Things (IoMT) to cloud services, application of RFID tags, Wireless Body Area Networks have proven effectiveness of new technologies in past epidemics. These technologies can provide monitoring capabilities for early detection of outbreaks and strengthening early warning system for public health issues. But, where the virus spread is rapid, we need efficient monitoring systems to collect and analyze real-time contact tracing, healthcare, and virus contamination data.

Epidemic issues range from outbreak control and quarantine monitoring to timely delivery of healthcare services. At the same time, information interaction with 3rd parties have become an indispensable part of epidemic services. Providing optimal and timely healthcare services based on telecommunication, widespread use of IoMT to essential public health systems, public insurance services, educational services in times of outbreak, all need secure and scalable information and communication infrastructure to keep pace with the massive amount of data being generated (16). Adetunji et al (17) elaborated on the Internet of Health Things (IoHT) and believed that application of IoHT can help in the management of COVID-19 diseases which entails quick diagnosis after recovery and during quarantine time.

Distributed ledger technology (DLT) such as Blockchain is a new paradigm in data management that relies on the concepts of secure data sharing through distributed ledgers and removing middlemen. Blockchain ensures a secure and transparent infrastructure with a minimum likelihood of manipulation through the distribution of data across the network and the decision to accept and consolidate data not through the central system approval but through the maximum consensus of full nodes in the network. The blockchain, provides a robust platform for tracking data inconsistencies and resisting data manipulation and tampering (18). Since the omnipresent data points and digital surveillance applications can easily exacerbate concerns about privacy and catastrophic consequences of the COVID-19 pandemic, adopting DLTs has been offered as a part of the healthcare ecosystem and Rapid Response Systems (RRS) due to the numerous benefits it offers (14). During the outbreak of COVID-19, many hospitals in China have used blockchain to be able to ensure the timely provision of medical services and accurate follow-up of patients (12).

The rising number of vaccine scams range from production process and fake clinical trials to abduct vaccine production formula. These threats remind of the need to develop or adapt appropriate information management infrastructures (19).

Regarding the mentioned issues, current study proposes a schema for a tamper-proof data management architecture during a pandemic. Therefore, the main objective is to present a blockchain-based CoviReader for controlling the spread of the disease while protecting their privacy (Fig. 1). The concept of CoviReader was first introduced in a paper by (20) as "a decentralized healthcare management system that shares user's data anonymously". They proposed a COVID-19 detector (reader) architecture based on a blockchain and QR Code architecture to facilitate detection and tracing of infected people.

Current article differently with the Cisneros and their colleagues, attempts to propose a CoviReader architecture for tracing the infected people while safeguarding people's identity while commuting in a presumably smart city.

To follow the goal, we have three challenges ahead:

i. Protecting citizen's identity by recording information with the digital identity;
ii. Ensuring that data recorded by healthcare centers are not manipulated;
iii. Communication in smart territories for quarantine control are effective and timely.

One of the notable challenges in blockchain architecture

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

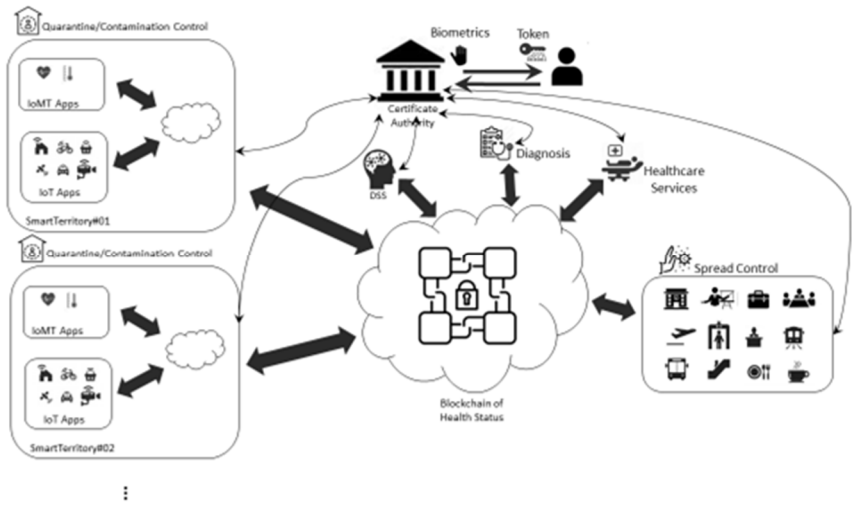

Figure 1. Basic Schema of Proposed Architecture

is the transactions per second (tps) rate. Concerning this matter, many solutions are introduced but the challenge of scalability (improving the rate of tps) in 1st and 2nd generation of blockchain is a growing concern (21-30).

In the following, we will take a closer look at the challenges of developing and selecting the right blockchain for the IoT ecosystem.

A. Scalability Trilemma

Known as scalability trilemma, the decentralization, scalability, and security are among important challenges of any distributed ledger infrastructure designed to implement real-world business cases. The scalability challenge in 1st gen blockchain was due to the size limit of each block and the proof of work (PoW) consensus mechanism (31). This "blockchain bottleneck" remained in 2nd gen (Ethereum) blockchains (32) (Fig. 2). In traditional blockchains with a single-chain architecture in which forking is prohibited, the consensus mechanism is one of the two main proof of stake (PoS) or PoW models used to slow down new block access to the blockchain and prevent new branch formation. This has become a bottleneck in transaction recording, especially in the IoT ecosystem which we will address.

Distributed ledgers in the heart of the blockchain record all issuing transactions of the network, and thus its architecture falls into the category of decentralized architectures. However, in this decentralized architecture, data manipulation is not possible and transactions in ledgers are tamperproof and not editable. In fact, the two sides of the scalability trilemma are well implemented in the 1st and 2nd gen blockchains, and according to Chauhan et al. (33), the fundamental challenge in this triad lies in the third side, i.e., scalability. Scalability means the ability of a system to accept an increasing number of elements or things (transactions, requests, etc.) to process the workload that is increasing or prone to increase (34). Chauhan et al. surveyed the challenge of blockchain infrastructure scalability since the birth of the Bitcoin network with a limit of 7 tps and the growing trend towards smart contracts and DAPPs and compared the solutions that meet the challenges (33).

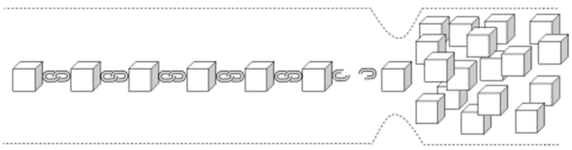

Figure 2. Blockchain bottleneck in traditional blockchains

Lightning protocol is one of the solutions introduced to increase the tps rate by defining and conducting the deals at the internal network level, aka. Off-chain (35).

The Sharding method was proposed as a nearly similar but on-chain solution to the scalability challenge by creating subnets that each have their own status and transaction history. Sharding solution dates to centralized databases and has a kind of layered data architecture in which data is segmented into independent databases, and each section hosts a database segment in its own dedicated server with its own local resources (36).

Finally, neither Bitcoin could overcome the scalability challenge in IoT ecosystem due to the high cost of its transactions and the violation of the blockchain constitution in the Lightning solution, nor did Sharding provide a clear guarantee to counter a 51% attack on a Shard and approve its corrupt transaction set. Chauhan considers the Sharding strategy to be a more appropriate solution because of its adherence to the values and constitutions of the blockchain. He notes that the challenge of scalability persists in 1st and 2nd generation blockchains, and that each solution adds a set of problems to the network (33).

Other solutions, such as RapidChain, were designed to solve the Bitcoin bottleneck (37). In RapidChain, which is a Shard-based approach, the consensus mechanism has been improved by forming a reference committee whose members are redefined at regular intervals called epoch.

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

Because the solution refers to the Kademlia routing protocol (38) between the client and the committee, the composition of the committee, whose members change regularly at epochs, prevents Sybil attack (39). Although, RapidChain offered a solution to improve the tps rate, it did not respond to the mining operations required for the consensus mechanism and the cost of the transactions. Del Monte et al. (40) claimed that their proposed solution for scalability trilemma does not compromise the fundamentals of blockchain and its security and decentralization. This research recommends setting up committees to make the necessary computations to approve transactions and add new blocks to the chain. Afterwards, much research with the proposal to optimize the PoW consensus mechanism and introduce PoS sought to improve the tps rate and increase scalability. Despite these innovative solutions, there is still no reliable way to break the consensus mechanism's dependence on mining operations and high transaction fees in 1st and 2nd gen blockchains.

IoT tools and sensors have limited resources that often not only fail to meet the mining perquisites required for the 1st and 2nd generation blockchain consensus mechanisms, but also low tps rates and long waiting times for confirmation of transactions, as well as the high transaction fees, are serious obstacles to deploy these generations of blockchain in the IoT ecosystem. Bin Cao et al. (41) examined the application of blockchain in the IoT ecosystem from four perspectives: trust, security, overhead, and scalability and pointed out the challenges of traditional blockchains in the IoT ecosystem from four aspects. The first one is the high energy consumption of blockchains for PoW and PoS consensus mechanisms and to validate new transactions, whereas in the IoT ecosystem with limited component resources, this consensus model is not optimal. The next issue was the cost of transactions in traditional blockchains, which causes low efficiency in micropayment ecosystems such as the IoT.

As the third aspect, transaction rate estimated at 7 tps in the 1st gen Bitcoin-based blockchain and 20 to 30 tps in the Ethereum-based blockchain, does not meet the high number of transactions generated in the IoT ecosystem. The fourth aspect was the delay in confirming transactions, which is inevitable due to the architecture of the traditional blockchains. This rate is 60 minutes in Bitcoin and 3 minutes in Ethereum, which is a very long time for IoT-based applications.

B. Blockchain in IoT Ecosystem Dilemma

Directed acyclic graph (DAG) structure has many usages in computer science. Replacing this structure with a blockchain structure by having the possibility of adding transactions simultaneously has a great impact on increasing the rate of operation in the blockchain. With the aim of improving scalability and tps rates, the 3rd generation of blockchain based on DAGs (42) were introduced. They are blockchains without blocks and without chains in which new transaction approval is subject to the approval of active network participants confirming one or more selected unconfirmed transactions. Using DAG in the 3rd generation of blockchain resolved the blockchain bottleneck and made it appropriate for using in IoT ecosystem (Fig. 3).

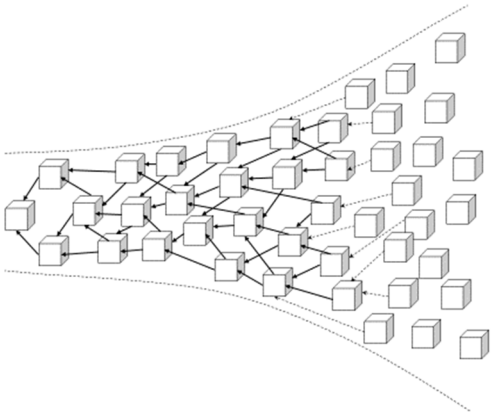

Figure 3. Tangle structure of 3rd gen DAG-based blockchains

IOTA Tangle is one example of a 3rd generation DAG-based blockchain in which each new transaction must confirm at least two previous transactions, where this selection is made in the first release of IOTA infrastructure based on the Monte-Carlo Markov chain algorithm (43). In the IOTA Tangle structure, transactions that are not yet fully confirmed are called "tips", and there are two general methods for selecting tips: a random algorithm, and a random selection navigation algorithm based on the Monte Carlo Markov chain in nodes of DAG. Monte Carlo Markov chain is used to approximate the posterior distribution of a parameter by random sampling in probabilistic space (44, 45).

The first method is subject to double spending attack, and the second is faced with the possibility of abandoning some transactions and creating orphan transactions, which of course is less risky compared with the consequences of the first method. Therefore, IOTA should solve the problem of orphan transactions.

Bin Cao et al. (41) conclude that DAG-based 3rd gen blockchains are faster and more cost-effective in confirming transactions than non-forking blockchains based on the mechanism of PoW or PoS consensus. Increase in transaction registration rates would lead to an increase in transaction confirmation rates, which can help increasing the rate of transaction confirmation during peak times. On the other hand, this will drastically reduce the speed of transaction confirmation during off-peak hours. They reminded that the choice of the basic version of IOTA in using a “coordinator” as a 3rd party to impose transactions with zero value on the network contradicts the nature of blockchain independence from the intermediation and its decentralization goal (41).

Ferraro et al (46) proposed an interesting solution to improve the tip selection algorithm for confirmation by the newcomer transaction. In this study an attempt has been made to prevent the transactions from being orphaned (never being selected) while avoiding the double-spending attack. Ferraro et al., with representing the constant α and the assumption that α is a positive value and v_x is equal to the accumulated weight of node X, introduce the probability of moving from transaction i to transaction j as a fraction of $f(-a(v_j-v_i))$. Now we have a variable called α that is very similar to the Boltzmann constant by Ferraro’s definition.

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

As the value of α increases, the number of orphan transactions increases, and if it tends to zero, as the orphan transaction rate reaches zero, the network is exposed to the risk of double spending. In this research, two steps have been proposed to manage this conflict: The first; Security step where choices made based on the Monte Carlo Markov chain and with a large amount of α, honest tips are preferred. And the second; Swipe step, which can be done both based on the Monte Carlo Markov chain selection algorithm and the random selection algorithm. But at this point α has a small value to ensure the selection of old and abandoned transactions. However, the "coordinator" was not the only problem with IOTA's infrastructure. The infrastructure has been the target of numerous attacks since 2018 (47-51), the most damaging in January 2018, when hackers stole $10 million worth of tokens from MIOTA (IOTA Cryptocurrency) users (51).

IOTA needed to develop a new version and fix the infrastructure problems to put the brilliant idea of creating the right blockchain for IoT ecosystem into a practical one, as well as to provide an effective way to counter attacks and fix its back holes. In this regard, IOTA foundation introduced the mechanism of Mana and automatic peering to counter Sybil and Eclipse attacks (52). Mana is a credit mechanism for IOTA network nodes in which each node that holds more tokens over a long period of time or exchanges tokens frequently in the network gains more credit in the network. In auto peering, instead of adding neighboring nodes based on the request and response process, the peering occurs automatically by the network and the addition of nodes to the network is managed. In this way, the possibility of sabotage and eclipse attack in the request and response process of peering is significantly reduced. In addition, to ensure that the data is not tampered, each node that records the information adds its public key to all signed transactions. Accordingly, other network nodes can verify the validity of the data logger node without having to maintain a list of node IDs (53).

The purpose of the IOTA development is to create a distributed ledger suitable for the IoT ecosystem, and the vision is to develop infrastructure with three main characteristics: scalability, lightness, and low transaction fee. IOTA efforts to eliminate the coordinator and strengthen the infrastructure led to introducing the Coordicide version in early 2020 and the first version was released by the end of that year (53). In this research, IOTA infrastructure Version 1.5 was used.

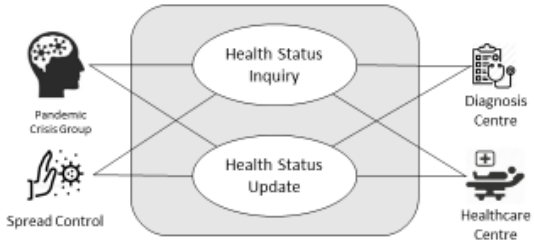

Figure 4. Use Case View

Methods

We proposed a system design to curb the pandemic while protecting the privacy of individuals. It is important to note that, according to the WHO, the key to control over prevalence of the COVID-19 pandemic is to quickly test and diagnose patients, enforce quarantine rules, and begin treatments (54). Therefore, we desire for a rapid-checking citizens' health status against clear signs of the disease and labeling them as healthy or diseased accordingly (Fig. 4).

Symptoms such as fever above 38 degrees and other symptoms (55), are being measured regularly in many places such as large shopping malls, schools, airports, etc. These considerations are good but not enough, though. A better strategy is taking COVID-19 test and then, ask people to show their COVID-19 test result at entries or gates. By referring people to diagnostic and healthcare centers, the COVID-19 test is taken, and the medical center is obliged to record and put the information online, so that they could be used by quarantine control authorities. A simple health status can be defined through 6 values according to Table 1.

Table 1. Description of health status

0	1	2	3	4	5
Healthy	Suspected	Confined	Quarantined	Infected	Expired

We propose every person must have a health status token kept in a Tangle. Due to the airborne prevalence of COVID-19 (4), outbreak control measures should be taken in crowded areas to check obvious signs of the disease (55) and update the people's token saved in a Tangle. Labeled as "suspected" means the last health status of a person is either not registered or "healthy" (Fig. 5).

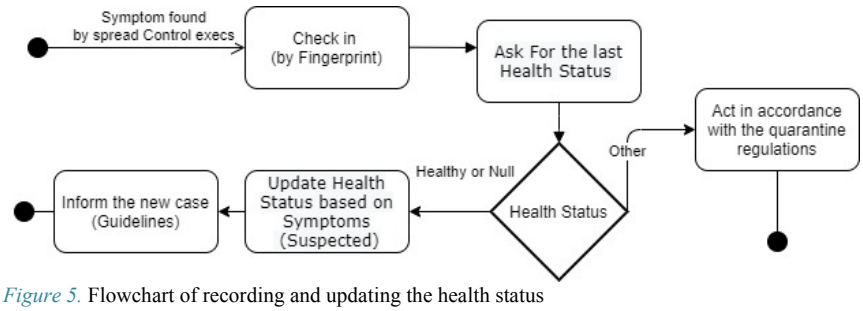

Figure 5. Flowchart of recording and updating the health status

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

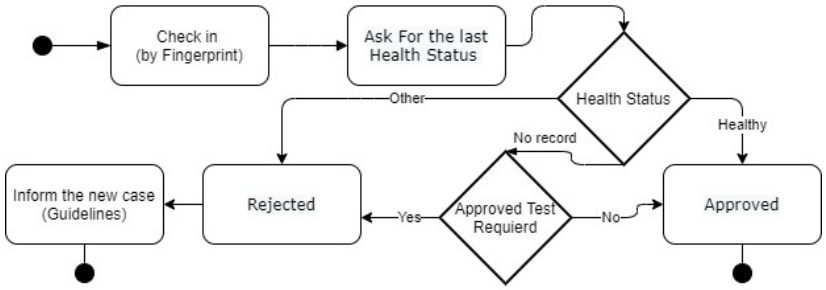

Figure 6. Flowchart of inquiring about people's health status

Health status inquiry of citizens with the aim of controlling the spread of the disease can be perform by a legal authority such as a police officer or by IoT a chip installed at the control gates. Accordingly, a pass will not be allowed if the Tangle status is "infected" or "suspected".

Figure 6 describes the process of inquiring about the latest health status from the Tangle.

Results

Implementation and Evaluation

Full nodes in IOTA have high computational capacity and are responsible for PoW processes for requests from nodes with limited resources, such as IoT nodes in the IoT ecosystem in smart territories. There is a rate control module responsible for blocking or penalizing a node that is recording transactions at a speed exceeding the network capacity. In the IOTA network infrastructure layer, the full node is configured with the Hornet tool. Each full node receives a transaction handled in IOTA as a message, then, registers the message if not stored in its local database. Next, it confirms the transaction and finally, sends the message to the neighboring nodes (53).

Figure 7 illustrates the proposed infrastructural layers. In the proposed architecture, a private Tangle is defined instead of a public network, and a web server is used to manage requests. Registered data on each full node extends to all network nodes with the Gossip protocol and is protected from alteration and tampering as soon as it is approved by Milestone. In fact, each full node in peering process associates with a set of neighboring nodes. IOTA infrastructure uses auto-peering to prevent eclipse attacks. Each node that records the information adds its public key to all signed transactions. This allows other nodes to verify the validity of the data logger node without having to maintain a list of node IDs in the database format. This occurs at the communication layer for the sole purpose of protecting the data from tampering, after which the data is not stored in the Tangle (56).

At the highest level, IoT tools in authorized centers are placed to record changes of the citizens' health status. Requests for registration, updates, and status inquiries are dispatched to the client through a webserver. The client communicates with the full node using the IOTA official client library. In case of registration and updating data, the information will be extended to the whole neighboring nodes

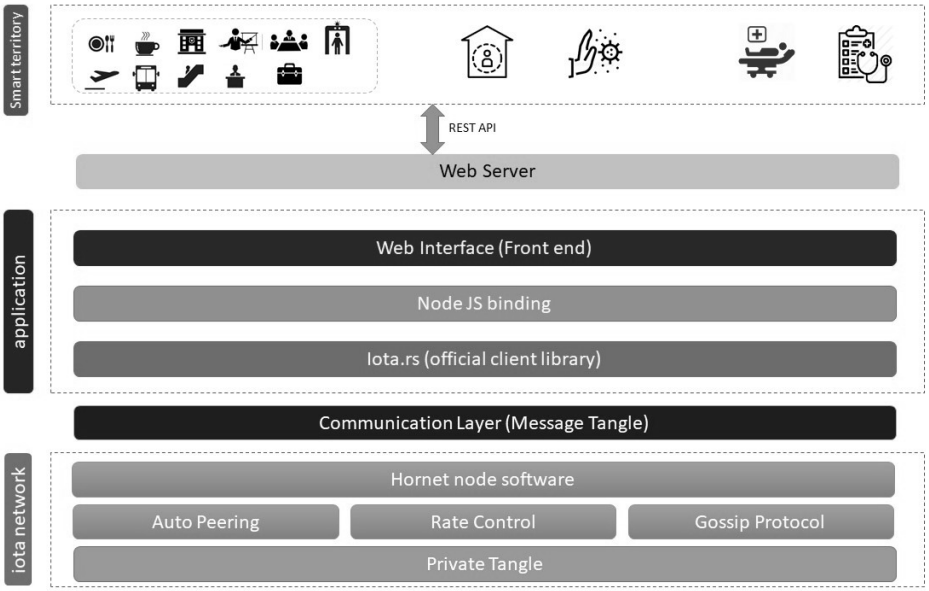

Figure 7. Top level view of architectural infrastructure layers (59)

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

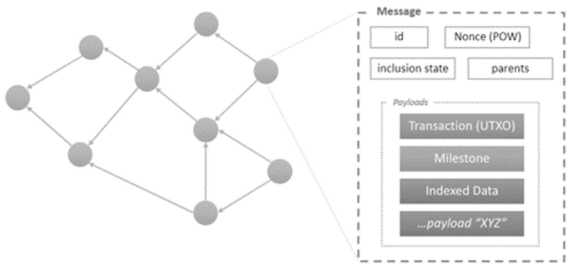

Figure 8. IOTA message structure (59)

and then to all network nodes. In case of inquiry, the latest status information will be sent to the client and transferred to higher layers based on which an appropriate decision is made to accept or reject the request.

Based on the needs of the prevalence control system, two general approaches in this view have been examined. The first approach is the transaction plan, which is developed based on the daily needs of registration and inquiry requests, and the second approach is the big data plan, which is based on the crisis management needs for data access and decision support. Both approaches are described in detail below.

A. Transaction Plan

The transaction plan includes all system data interactions in registration and inquiry requests. The limited resources of IoT components for processing in smart territories and the need for high registration and retrieval rates are considered in this approach. Each transaction in the system is distributed as a "message" in the IOTA Tangle and approves by the network. Each message has its own unique number (id) through which can be accessed. The message structure in the IOTA network is shown in the Figure 8.

In the proposed structure, each message is connected to at least two and up to eight previous messages, and any change in this message will invalidate the message by invalidating the attached message chain. The Iota network guarantees that the message will not be tampered as soon as the message is approved by Milestone, which takes about 8 seconds (56). Each message stores in binary format and can hold up to 32 KB of information. In the present study, the message structure has been proposed to store people's information in Tangle.

B. Big Data Plan

Big data plan is proposed to access aggregate information and interactions of citizens in the smart territories during the pandemic. The process of fetching and aggregating daily information by the Decision Support Service (DSS) provider has been shown in Figure 9. Each IOTA full node gathers the last day information at off-the-peak time and records its hash code in the Tangle. The hash operation is performed by SHA-256 algorithm (256 Bits) which is fully consistent with the data size limit in IOTA message's structure. Due to the data size limit in Tangle messages (32k), each data file is spilt into 28KB parts and stored in the Tangle with its hash ID. The DSS provider, then, fetches a list of all available hashes from the Tangle and compiles the file for each registered block for each hash. In this way, the DSS provider at crisis headquarters will gather and aggregate information. Besides, it is better to consider the time interval to make sure that the nodes have enough time to execute the hash generation process and register the blocks. As shown in the Figure 9, the DSS server collects the file blocks by fetching the messages of each hash identifier, and after retrieving the file, it will also be able to validate it with the hash code. Now, with the daily information file, the DSS server has access to last day's information for every node. This aggregate information will only be provided to the crisis headquarters to make decisions based on privacy

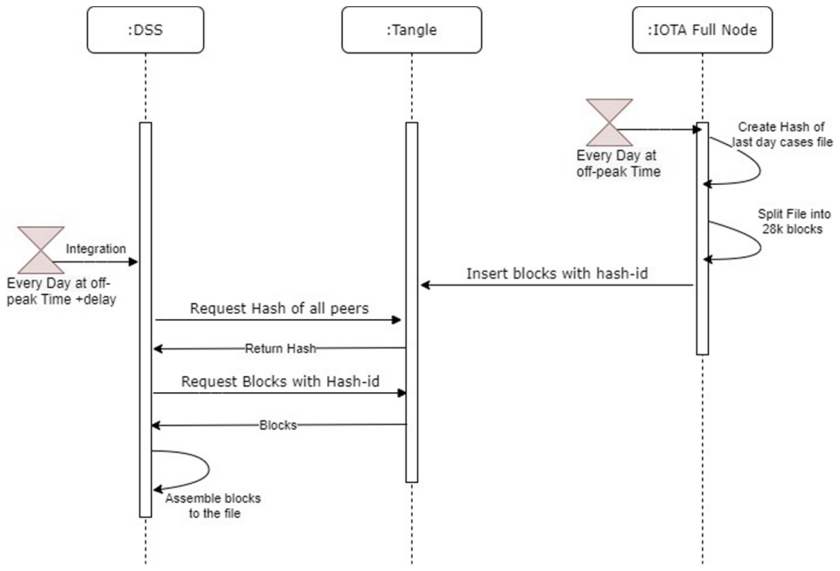

Figure 9. Process of fetching and aggregating data by the DSS provide

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

rights and the extent of access to 3rd party information. Afterwards, the COVID-19 crisis headquarter can identify hotspot zones of the disease and make decisions about the infected people and their relatives and colleagues, while necessary. By using this aggregated information numerous reports including combination of aggregate health status data and 3rd party data sources (i.e., from registration, social security, intercity traffic, etc.) are available at the headquarters. In fact, a DSS will be used to prepare analytical reports in smart territories.

The level of information provided by diagnostic and healthcare centers for the pandemic crisis headquarters can be different from the usual data for controlling the outbreak. It is also possible for medical centers to record more information in the data file, for example, including data received from reference laboratories on the identification of different variants of the virus and the severity of the disease and additional information on this matter. These data, which are stored in a coordinated JSON format and then hashed and encrypted, will only be provided to the crisis headquarter. Furthermore, verification of the validity of the final file against data manipulation will also be possible by comparing the hash of the consolidated received file with the original hash of the file registered in the Tangle.

Deployment

In this section, we tested the CoviReader architecture for deployment of different layers. The connection between spread control and medical centers that inquire and update the health status of citizens is shown in the Figure 10. The registration and inquiry request are sent to the web server and from there to the full node of the IOTA network. The private Tangle has no limit on peering the number of full nodes, and the web service provider for different areas also needs to be connected to the full node in their areas.

Moreover, it is possible for IoT components to interact with the network to achieve desired data and response timely and appropriately to citizen's requests (Fig. 11). Before setting up any full node, it is necessary to set up secure SSH login and disable unnecessary ports. While all citizen information is encrypted and stored, the same data is stored on all nodes.

At this architecture, the COVID-19 crisis headquarter needs to access the IOTA infrastructure to update health status information, combine specific pandemic data received from medical and outbreak control centers, and to

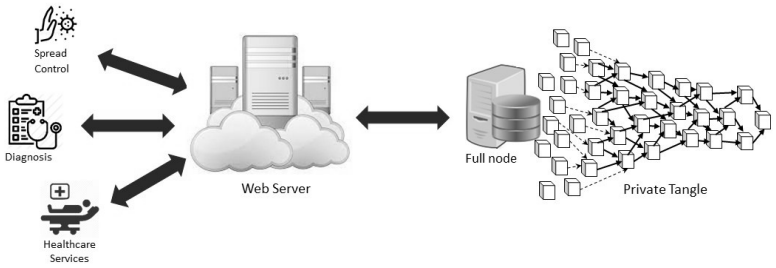

Figure 10. Architecture of communication between IOTA and authorities in smart territories

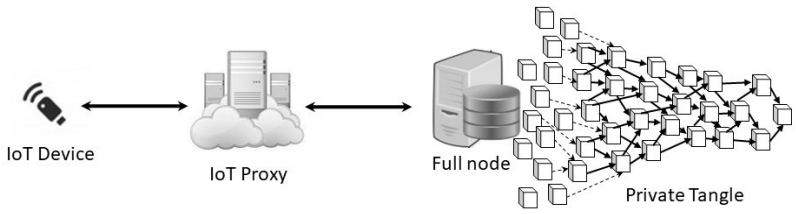

Figure 11. Architecture of communication between IOTA and IoT

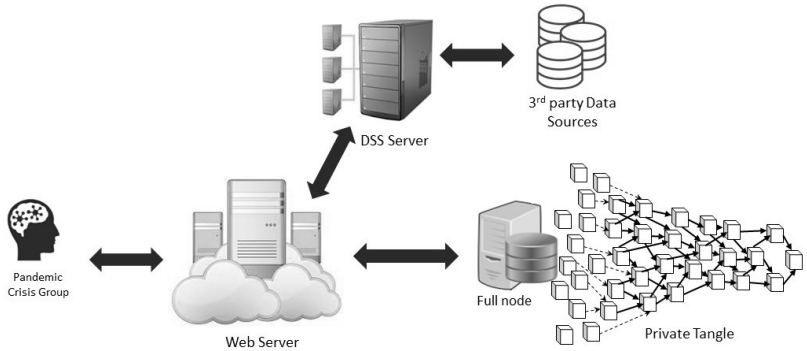

Figure 12. Architecture of communication between the DSS, Tangle and 3rd party data sources

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

connect to 3rd party data sources (Fig. 12).

It should be mentioned that that only the crisis headquarters will have access to the data of the DSS server. Figure 12 illustrates the connections among the DSS of the COVID-19 crisis headquarters and other components for information aggregation, registration and updating.

Conclusion

The proposed CoviReader architecture ensures the availability of the people's health status data and at the same time constrains manipulation or disclosure of that data. The catastrophic consequences of the COVID-19 pandemic led us to propose application of this architecture as a transparency-enhancing solution. Compared to other health status control tools like (20), the proposed CoviReader benefits from an anti-information disclosure architecture under a fast IOTA tangle to deliver the information to the healthcare headquarters. It is inevitable that the architecture is deemed to become an integral part of the future healthcare ecosystem due to the numerous benefits it offers. While implementing the architecture in IoT ecosystem with limited capability of sensors is a challenge, appropriate sensors should be used to monitor patients with chronic diseases or under surveillance persons beyond the pandemic situations.

Acknowledgement

This article is extracted from the first author MSc dissertation supervised by the second and the third authors.

Conflict of Interests

The authors declare that they have no competing interests.

References

1. Arshad Ali S, Baloch M, Ahmed N, Arshad Ali A, Iqbal A. The outbreak of Coronavirus Disease 2019 (COVID-19)—An emerging global health threat. J Infect Public Health. 2020;13(4):644-6.
2. WHO. Opening remarks at the media briefing on COVID-19 2020 [Available from: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.
3. STATISTA. Global number of connected IoT devices 2030. 2023.
4. WHO. Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations. 2020.
5. Iserson KV. Principles of biomedical ethics. Emerg Med Clin North Am. 1999;17(2):283-306.
6. Cavalera C. COVID-19 Psychological Implications: The Role of Shame and Guilt. Front Psychol. 2020;11:571828.
7. Kelleher SR. Some Air Passengers Are Faking Negative Covid-19 Test Results, Per U.K. Reports. Forbes. 2020.
8. Campbell J. FBI warns companies of employees faking coronavirus test results. 2020. [Available from: https://www.cnn.com/2020/04/14/politics/fbi-warning-fake-coronavirus-test-results/index.html]
9. Illmer A. Singapore reveals Covid privacy data available to police. BBC NEWS. 2021. [Available from: https://www.bbc.com/news/world-asia-55541001
10. Kamel Boulos MN, Peng G, VoPham T. An overview of GeoAI applications in health and healthcare. Int J Health Geogr. 2019;18(1):7, s12942-019-0171-2.
11. Shahidul Islam M, Islam MT, Almutairi AF, Beng GK, Misran N, Amin N. Monitoring of the Human Body Signal through the Internet of Things (IoT) Based LoRa Wireless Network System. Appl Sci. 2019;9(9):1884.
12. Ting DSW, Carin L, Dzau V, Wong TY. Digital technology and COVID-19. Nature Med. 2020;26(4):459-61.
13. Sharma PK, Park JH. Blockchain based hybrid network architecture for the smart city. Future Gener Comput Syst. 2018;86:650-5.
14. Chamola V, Hassija V, Gupta V, Guizani M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. IEEE Access. 2020;8:90225-65.
15. Sareen S, Sood SK, Gupta SK. IoT-based cloud framework to control Ebola virus outbreak. J Ambient Intell Humaniz Comput. 2018;9(3):459-76.
16. Allam Z, Jones DS. On the Coronavirus (COVID-19) Outbreak and the Smart City Network: Universal Data Sharing Standards Coupled with Artificial Intelligence (AI) to Benefit Urban Health Monitoring and Management. Healthcare. 2020;8(1):46.
17. Adetunji CO, Olaniyan OT, Adeyomoye O, Dare A, Adeniyi MJ, Alex E, et al. Internet of Health Things (IoHT) for COVID-19. Diabetes Metab Syndr. 2022:75-87.
18. Hassan MU, Rehmani MH, Chen J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Gener Comput Syst. 2019;97:512-29.
19. Peng S, Hu X, Zhang J, Xie X, Long C, Tian Z, et al. An Efficient Double-Layer Blockchain Method for Vaccine Production Supervision. IEEE Trans NanoBiosci. 2020;19(3):579-87.
20. Cisneros B, Ye J, Park CH, Kim Y, editors. CoviReader: using IOTA and QR code technology to control epidemic diseases across the us. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC); 2021: IEEE.
21. Li W, Feng C, Zhang L, Xu H, Cao B, Imran MA. A Scalable Multi-Layer PBFT Consensus for Blockchain. IEEE Trans Parallel Distrib Syst. 2021;32(5):1146-60.
22. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24(6):1211-20.
23. Mazlan AA, Mohd Daud S, Mohd Sam S, Abas H, Abdul Rasid SZ, Yusof MF. Scalability Challenges in Healthcare Blockchain System—A Systematic Review. IEEE Access. 2020;8:23663-73.
24. Worley C, Skjellum A, editors. Blockchain Tradeoffs and Challenges for Current and Emerging Applications: Generalization, Fragmentation, Sidechains, and Scalability. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018 7/2018. Halifax, NS, Canada: IEEE.
25. Meinert E, Alturkistani A, Foley KA, Osama T, Car J, Majeed A, et al. Blockchain Implementation in Health Care: Protocol for a Systematic Review. JMIR Res Protocol. 2019;8(2):e10994.
26. Sanka AI, Cheung RCC, editors. Efficient High Performance FPGA based NoSQL Caching System for Blockchain Scalability and Throughput Improvement. 2018 26th International Conference on Systems Engineering (ICSEng); 2018 12/2018. Sydney, Australia: IEEE.
27. Zhou Q, Huang H, Zheng Z, Bian J. Solutions to Scalability of Blockchain: A Survey. IEEE Access. 2020;8:16440-55.
28. Liang W, Tang M, Long J, Peng X, Xu J, Li K-C. A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things. IEEE Trans Industr Inform. 2019;15(6):3582-92.
29. Ajorlou A, Abbasfar A, editors. An Optimized Structure of State Channel Network to Improve Scalability of Blockchain Algorithms. 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC); 2020 2020-9-9. Tehran, Iran: IEEE.
30. Qin Q, Jin B, Liu Y. A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain. BioMed Res Int. 2021;2021:1-14.
31. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentral Bus Rev. 2008 Oct 31:21260.
32. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014;151(2014):1-32.
33. Chauhan A, Malviya OP, Verma M, Mor TS, editors. Blockchain and Scalability. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C); 2018 7/2018. Lisbon: IEEE.
34. Hill MD. What is scalability? ACM SIGARCH Comput Archit News. 1990;18(4):18-21.
35. Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]

instant payments. [Available from https://lightning. network/lightning-network-paper. pdf. 2016 Jan].
36. Ravi Kumar Y, Basha N, Kumar KMK, Sharma BM, Kerekovski K, Ravi Kumar Y, et al. Oracle Sharding: Oracle High Availability, Disaster Recovery, and Cloud Services: Explore RAC, Data Guard, and Cloud Technology. Springer; 2019:335-98.
37. Zamani M, Movahedi M, Raykova M, editors. RapidChain: Scaling Blockchain via Full Sharding. CCS '18: 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 2018-10-15. Toronto Canada: ACM.
38. Maymounkov P, Mazieres D. Kademlia: A peer-to-peer information system based on the xor metric. Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers: Springer; 2002. p. 53-65.
39. Patil HK, Chen TM. Wireless Sensor Network Security. Computer and Information Security Handbook: Elsevier; 2017. p. 317-37.
40. Monte GD, Pennino D, Pizzonia M, editors. Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma. Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems; 2020.
41. Cao B, Li Y, Zhang L, Zhang L, Mumtaz S, Zhou Z, et al. When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. IEEE Network. 2019;33(6):133-9.
42. Pervez H, Muneeb M, Irfan MU, Haq IU, editors. A Comparative Analysis of DAG-Based Blockchain Architectures. 2018 12th International Conference on Open Source Systems and Technologies (ICOSST); 2018 12/2018. Lahore, Pakistan: IEEE.
43. Popov S. The tangle. White paper. 2018;1(3):30.
44. Fearn T, Gelman A, Carlin JB, Stern HS, Rubin DB. Bayesian Data Analysis. Biometrics. 1996;52(3):1160.
45. McGrayne SB. The Theory That Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarines, & Emerged Triumphant from Two Centuries of C: Yale University Press; 2011.
46. Ferraro P, King C, Shorten R. On the Stability of Unverified Transactions in a DAG-Based Distributed Ledger. IEEE Trans Automat Contr. 2020;65(9):3772-83.
47. Colavita M, Tanzer G. A cryptanalysis of IOTA's curl hash function. White paper. 2018. p. 1-13.
48. Shafeeq S, Zeadally S, Alam M, Khan A. Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach. IEEE Trans Eng Manag. 2020;67(4):1244-55.
49. Perazzo P, Arena A, Dini G, editors. An Analysis of Routing Attacks Against IOTA Cryptocurrency. 2020 IEEE International Conference on Blockchain (Blockchain); 2020 11/2020. Rhodes Island, Greece: IEEE.
50. De Roode G, Ullah I, Havinga PJM, editors. How to Break IOTA Heart by Replaying? 2018 IEEE Globecom Workshops (GC Wkshps); 2018 12/2018. Abu Dhabi, United Arab Emirates: IEEE.
51. Heilman E, Narula N, Tanzer G, Lovejoy J, Colavita M, Virza M, et al. Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency. IACR Trans Symmetric Cryptol. 2020:367-91.
52. Singh A, Ngan T-W, Druschel P, Wallach DS, editors. Eclipse Attacks on Overlay Networks: Threats and Defenses. Proceedings IEEE INFOCOM 2006 25TH IEEE International Conference on Computer Communications; 2006 2006. Barcelona, Spain: IEEE.
53. Popov S, Moog H, Camargo D, Capossele A, Dimitrov V, Gal A, et al. The coordicide. White paper. 2020:1-30.
54. Hove EF. The Complexities of Public Health Communication on COVID-19 Vaccination in the Social Media Era: Implications on Zimbabwe's Health System. The COVID-19-Health Systems Nexus: Emerging Trends, Issues and Dynamics in Zimbabwe: Springer; 2023. p. 259-75.
55. Dennison Himmelfarb CR, Baptiste D. Coronavirus Disease (COVID-19): Implications for Cardiovascular and Socially At-risk Populations. J Cardiovasc Nurs. 2020;35(4):318-21.
56. Fotia L, Delicato F, Fortino GJACS. Trust in edge-based internet of things architectures: state of the art and research challenges. ACM Comput Surv. 2023;55(9):1-34.

[Downloaded from mjiri.iums.ac.ir on 2026-11-09]

[DOI: 10.47176/mjiri.36.180]