Research Article

International Journal of Advanced Technology and Engineering Exploration, Vol 10(106)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2023.1010184

Trusted surveillance system based on blockchain-internet of spatial things for smart cities

Noor Alsaedi* **and Ali Sadeq Abdulhadi Jalal**
Department of Information and Communication Engineering, College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Received: 20-June-2023; Revised: 25-September-2023; Accepted: 27-September-2023

Abstract
Technological advancements in smart cities are a global trend, primarily focused on enhancing the quality of life for citizens while also monitoring urban environments. Viewing smart cities as urban surveillance platforms, there arises a pressing need for efficient analysis and storage of video streams from numerous cameras scattered across the city, owned by various stakeholders. However, surveillance systems face several internet of things (IoT) challenges, including privacy concerns, scalability issues, and substantial energy consumption. To tackle these challenges, the development of a trusted video surveillance system by integrating the internet of spatial things (IoST) with fog computing and blockchain technology was introduced. Fog nodes are strategically deployed at the network's edge, enabling the extension of cloud services closer to the data source. This deployment strategy aims to reduce latency and alleviate network congestion. At these fog nodes, the system employs a proof-of-work-based consensus algorithm, encrypted using the secure hash algorithm (SHA-256), to ensure data trust and reliability within the blockchain infrastructure supporting the surveillance system. The evaluation of our proposed blockchain-IoST surveillance system involves a comparison of two case studies: one based on fog computing and the other on traditional cloud-based blockchain-IoST implementations, conducted within the iFogSim framework. Furthermore, the system's scalability is tested under various scenarios. To assess the effectiveness of our methodology in mitigating latency, optimizing network utilization, and reducing energy consumption, we conducted comprehensive simulations. The results of our experiments clearly demonstrate the advantages of the fog-based blockchain-IoST approach. This approach significantly reduces latency and network utilization when compared to the conventional cloud-based blockchain-IoST implementation in the trusted video surveillance system. Additionally, the findings indicate that adopting the fog-based blockchain-IoST approach leads to a noteworthy reduction in energy consumption compared to the cloud-based implementation, further enhancing the sustainability and efficiency of the surveillance system.

Keywords
Video surveillance system, Internet of spatial things, Spatial blockchain, Fog based blockchain-IoST, Cloud based blockchain-IoST.

1.Introduction
Nowadays, smart cities are a result of frequent technological advancements that improve the quality of life for their residents [1]. For smart cities, video surveillance is an important application in private and public sectors to monitor and protect areas at different scales which brings many problems and challenges, such as security and privacy of data that is collected from heterogenous sources [2].

Furthermore, many video events, a lack of quality, a significant transmission latency for video data, and the loss of video surveillance data integrity [3]. Moreover, these systems still lack precision for real-time reactions that may be delayed. In addition, environmental variations are a constraint for any system. These obstacles are problematic for video surveillance systems. By analyzing and comprehending the recorded videos, the processing of data using several proposed algorithms may aid in avoiding these issues through analysis and comprehension [2].

The smart city is a significant application of the internet of things (IoT) and is predicted to connect

*Author for correspondence

over 30 billion things by 2025 [4–6]. Furthermore, IoT supports real time communication among various remote devices, people, and environments [7]. Thus, the IoT may experience new challenges with security, privacy, and scalability [8]. In addition, the stored videos are vulnerable to access by unauthorized persons because of insecure techniques for data storage and sharing [9].

Most of the existing IoT platforms are based on cloud computing for data processing due to their capabilities in the storage and processing of big data. However, major challenges with this kind of platform are latency, security, and privacy [10, 11]. Fog computing, a distributed computing paradigm, was developed to expand the communication, process, and storage capability to the network's edge [12]. The distributed environment of fog computing base IoT drives the necessity to deploy distributed security mechanisms to protect data transactions and network resources [13]. Blockchain has been recognized as one of the significant technologies since the advent of the internet. It is distributed ledger technology (DLT) that supports fog based IoT platforms to provide decentralized and distributed trusted and secure solutions. Moreover, it is an immutable database ledger as a result of utilizing cryptographic mechanisms. Two types of cryptography are frequently used with blockchains; one-way hashing functions like secure hash algorithm-256 (SHA-256) and two-way functions like asymmetric encryption utilizing public and private keys [11, 14]. Hash functions permit the instantaneous generation of hash values for all data and the avoidance of conflicts, as each hash value is distinct based on the input data [15]. The consensus algorithm is a crucial component of blockchain technology as it is used for the decision-making process among blockchain nodes in the network. However, there have been many consensus methods developed such as proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), practical byzantine fault tolerance (PBFT), and ripple [16], and each method has its own performance and security features [17]. Therefore, it is imperative to select a consensus protocol that fulfills the specific requirements of the application. The PoW algorithm is the most popular consensus algorithm, having been introduced with Bitcoin by Nakumoto in 2008 [18]. The validation of each block is performed in a distributed manner using a consensus algorithm executed by certain network nodes known as miners [19]. The algorithm is based on difficult-to-compute but easy-to-verify mathematical problems. It makes the problem computationally expensive in a manner that reduces the likelihood of nodes simultaneously computing the same block, thereby decreasing the possibility of forks. In addition, in many consensus methods, such as PoS, the miner with a greater stake possesses a higher degree of control over the network. PoW grants equal opportunity for all miners to mine a block, with the reward going to the miner who conducts the most computations [17, 20].

Till now researchers have not put much effort into recognizing the challenges and possibilities offered by blockchain for video-streaming applications [21]. To face the above shortcomings and risks, we propose a blockchain-IoST framework for a video surveillance system with considering the next generation network technologies by utilizing blockchain in fog computing to produce an efficient and trusted surveillance system. The suggested system comprises three layers which are the spatial data source layer (L1), fog layer (L2), and cloud layer (L3) as illustrated in *Figure 1*. The fog nodes are implemented at the edge of the network and are accessed via the Internet. Whereas, the cloud node is located away from users. For each area, the fog node receives recorded video frames from intelligent cameras continually for processing.

The main contributions of this paper are as follows:

1. Build a three-layered internet of spatial things (IoST) framework. L1 comprises the sources of spatial data. Fog computing is applied at L2. L3 represents the cloud layer for achieving an efficient infrastructure concerning latency, energy consumption, and network usage.
2. Install distributed smart camera networks at L1 to implement an intelligent surveillance system.
3. Apply PoW consensus protocol to verify blockchains based on SHA-256. Encrypted video frames are distributed and stored at L2 to overcome privacy and security problems of the saved data.
4. Evaluate the suggested surveillance system's efficacy and efficiency in fog based blockchain-IoST placement through iFogSim simulation with scalability, latency, network utilization, and energy consumption.

The structure of this paper is as follows. Section 2 explores related work conducted in the field of our study. Section 3 illustrates the proposed approach as well as its architecture, algorithm and experimental configuration. Section 4 analyzes the efficiency and scalability of the proposed system. It also highlights

the research challenges. Finally, section 5 concludes this work with future research directions.

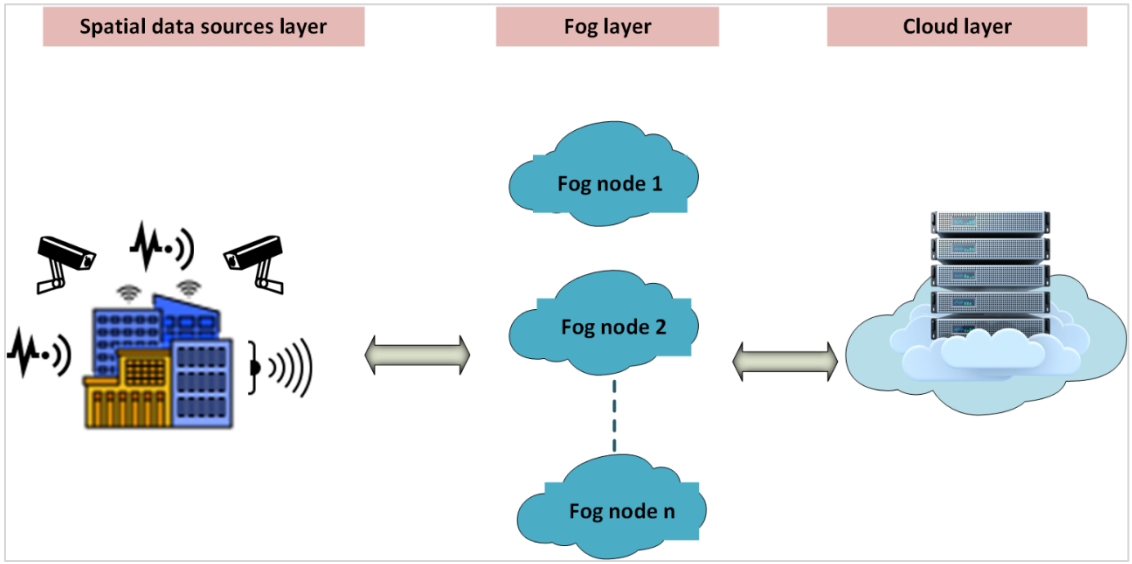

Figure 1 Fog based Blockchain-IoST architecture for a video surveillance system

2.Literature review

Extensive prior research has been conducted in this area of video surveillance systems. Numerous prior studies have engaged with diverse technological platforms. Xu et al. [22] proposed a semantic-based paradigm called video structural description (VSD) to effectively express and organize the content within the videos. The utilization of big spatio-temporal data has been employed to identify and analyze patterns of surveillance inside urban environments. The platform for organizing surveillance videos with cloud enhancement is also provided. This paper presents a comprehensive analysis of individuals and vehicles in surveillance videos using VSD techniques in the context of public security. However, the current method lacks effectiveness in terms of real-time responsiveness. Chen et al. [23] proposed an intelligent urban surveillance solution based on fog computing. Using traffic monitoring as a case study, the proposed fog computing-based system can track speeding vehicles and acquire real-time speed data. In the experimental prototype, tracking duties for each vehicle in video frames are distributed to onsite fog nodes. The study used large amounts of data collected by a drone acting as a camera sensor in the sky to observe areas of interest. Even though the initial findings are promising, the study consumes a significant number of computational resources. Memos and Psannis [24] introduced a clever surveillance system based on unmanned aerial vehicles (UAVs) that can be used in a wireless sensor network (WSN) for data collection. Moreover, energy harvesting (EH) techniques can also be used in parallel to offer energy efficiency (EE) and extend the network lifetime. Since sensor nodes can be applied to inaccessible environments such as glaciers and rugged mountains, UAVs can be used as a data collector mobile sink to collect all obtained information and send it to a cloud server before delivering it to an IoT device. For optimized results, additional research is required, as is the integration of data mining technologies such as artificial intelligence (AI) and machine learning (ML) to WSNs and cloud servers.

The developing 5G technology presents significant standards in the field of telecommunication and addresses the limitations encountered by conventional mobile networks through the provision of uninterrupted network connectivity. The technology facilitates the implementation of innovative business approaches and a wide range of vertical applications by improving network capacity, enhancing throughput, and ensuring good quality-of-service [25–27]. To design effective and secure fifth generation (5G)-enabled applications for smart cities, blockchain based IoT draws the great attention of researchers due to its advantages, especially the secure communication of transactions, immutable data storage, and decentralized nature [12]. Rego et al. [28] introduced an intelligent surveillance system that incorporates advanced technologies within an IoT framework, which is interconnected via a software-defined networking (SDN) infrastructure.

The proposed system involves the automatic recording and secure storage of video data within a blockchain framework. Subsequently, the video data is subjected to analysis and interpretation by computer vision techniques, specifically those based on deep learning. This process is executed either through edge computing or cloud computing. The system implements certain procedures in order to ensure the provision of quality of service (QoS) and quality of experience (QoE). Additionally, the system has passed testing in many scenarios. Various investigations and research are conducted to develop surveillance systems using blockchain technology. The research carried out in [29] suggested a trusted video surveillance system based on the blockchain system. Videos generated from internet protocol (IP) cameras are encrypted and saved in inter planetary file system (IPFS) via a private blockchain network built by trusted administrators. IP cameras are a type of digital video cameras that are mainly installed in various settings for the purpose of surveillance. These cameras have the capability to transmit their recorded data over the internet, enabling remote access [30]. The suggested model's efficiency in terms of network costs and security against intrusion still needs to be evaluated by the system. The preservation of security and privacy represents critical concerns within the realm of video surveillance.

Fitwi and Chen [31] investigated the utilization of blockchain-based systems for ensuring the integrity of stored data from closed-circuit television (CCTV) cameras in smart cities. This approach aims to prevent any unauthorized modification or manipulation of the recorded information. The utilization of blockchain metadata enables the facilitation of data retrieval from digital surveillance systems, hence aiding law enforcement agencies and clients in ensuring the security of recorded information. This proposal suggests the implementation of a private blockchain system integrated with a very effective video frame encryption method. The objective is to facilitate the secure and privacy-conscious sharing of stored surveillance video. The privacy of data is growing as a significant issue in the domains of blockchain technology [32] and video surveillance [33]. Upmanyu et al. [33] proposed a secure framework to carry out privacy preserving surveillance. The approach is derived from a secret sharing scheme based on the Chinese Remainder theorem, suitably adapted to image data. It works well with computing/storing on remote server clouds.

Blockchain technology plays a crucial role in ensuring data integrity within various systems, including the management of medical records and the monitoring of gas consumption in intelligent urban environments [34–36]. Gallo's experimental work [37] illustrated how to ensure the integrity of surveillance videos for smart cities. He employed a blockchain-based IoT to ensure integrity by sending hash block information to blockchain networks that all connected devices can trust. The preservation of camera settings plays a crucial role in protecting privacy since it enables individuals to monitor any violations upon their personal privacy. In addition, the proposed system gives camera settings validity and immutability. Yet, the recommended method may investigate to evaluate their privacy.

Similarly, the work in [38] suggested blockchain based IoT surveillance system for smart cities to manage, store, and verify the CCTV cameras. The system collected the data from CCTV cameras and sensors, applied blockchain technology to verify CCTV videos and detect forgery videos, then data was stored in distributed nodes. Due to the incentive mechanism, the system must reduce the consumed bandwidth. Moolikagedara et al. [39] developed and deployed a surveillance system that utilizes blockchain technology to build communication among vehicles in a smart city. The research broadened the range of video surveillance data collection for observational purposes, resulting in improved situational awareness. This was achieved by establishing a connection between video frames obtained through intelligent surveillance systems and blockchain technology. In order to enhance the dependability of the system, the combination of two cryptographic functions, namely hashing and signing, is utilized in conjunction with blockchain technology. The integration of this technology guarantees the implementation of secure and tamper-proof solutions for the current intelligent surveillance system. This study has a constraint related to the requirement of maintaining a minimum number of connected nodes in order to improve the system's availability. Furthermore, it should be noted that this approach lacks resistance against potential quantum computer attacks. The surveillance systems based IoT may be developed to serve dedicated applications. Of these studies, [40] illustrated how to use blockchain technology for surveillance systems in a smart health environment. The system monitors disease in public locations instead of individuals considering the time of the infection. Pane et al. [41] designed a surveillance system based blockchain with a proof of

authority consensus mechanism besides the suggested step-wise implementation process to develop postmarket surveillance (PMS) system for medical devices. It benefits all parties participating in the process, encompassing new regulatory measures, and has several benefits. It benefits all parties participating in the process, encompassing support for new regulatory efforts. Despite the suggested system focuses on data privacy, storage, exchange, and standardization solutions, it has to handle a blockchain-based safety monitoring medical devices system. To address the vulnerability and ensure IoT security, researchers in [42] presented a consensus algorithm and multi-layer IoT-based blockchain model. The suggested system was lightweight as it operated the access control for the IoT chain data using a Hyperledger fabric-based monitoring chain layer. However, the system needs to improve network routing and decrease network latency. As a first step towards building a smart city, researchers in [43] introduced a smart district platform using blockchain based IoT. The proposed model has an efficient energy management system. Unfortunately, the system must be extended to connect many more devices and blockchains taking into account every factor to enhance life quality of citizens.

With the increasing utilization of spatial data and the continuous upgrading of blockchain architecture, the demand for spatial blockchain platforms to serve a trusted decentralized application has emerged rapidly as suggested in [44] for trading, [14, 45] for health applications. The positioning of an object in space is referred to as its spatial characteristics and spatial data is presented on a map in the form of geographic coordinates [46, 47]. The research carried out by Eldrandaly et al. [48] developed the IoST as an integrated framework connecting smart devices with an emphasis on gathering spatial data on objects. Li et al. [49] developed a framework for secure surveillance in smart cities. The implementation of a secure authentication protocol that can resist man-in-the-middle (MITM) and replay attacks. In this work, we developed a model for secure video surveillance with four participants: a trusted authority (TA), a media cloud, a monitor, and a camera. the system constructed a video security decryption software based on transparent encryption. All system-installed cameras and users who wish to view the video data must register with a TA and acquire a unique key. Yet, the system may optimize the video encryption scheme in order to increase the encryption efficacy and decrease the encryption consumption in the cameras. In general, these studies highlight the necessity of implementing surveillance systems in smart cities, particularly those that employ state of art technologies. This study introduces a trust video surveillance system, which has been the object of little academic research. Specifically, the focus is on enhancing QoS within smart cities and considering the privacy and security issues.

3.Methods

3.1Proposed architecture

The proposed fog based blockchain-IoST architecture comprises three layers as shown in *Figure 1*. L1 has intelligent cameras, microcontrollers, and LEDs. Intelligent video cameras are positioned above their site of view (SoV) and output recorded videos. L2 of the suggested system is a fog node that is connected to the cameras via a microcontroller device and to L3 through a proxy server. The resultant commands and the information are sent to actuators after processing the video frames at the fog nodes. Fog nodes are connected to L3 via a proxy server. In the proposed architecture, video frames are securely encrypted, stored, and exported safely at L2. *Figure 2* illustrates the comprehensive workflow of the proposed system.

3.2Implementation of the proposed method

Implementing functionalities of fog base blockchain-IoST enables us to solve the main problems of centralized surveillance systems, especially: privacy, scalability, integrity, and safe storage. The operation process started from L1 where distributed intelligent video cameras are installed to cover their SoV and continuously send captured video frames for processing at L2. Secondly, fog nodes track the moving objects from the video frames that come from multiple cameras then it calculates the coordinates of the tracked objects. Following that, the spatial data of the objects are subject to blockchain technology to generate a spatial blockchain through a PoW protocol. Eventually, each fog sends spatial blockchain data backup to the cloud. The trusted video surveillance system algorithm describes the flow of the work.

Algorithm: Trusted video surveillance system

1. Input: video stream
2. Output: spatial blockchain
3. Begin
4. initialize the system
5. Set video cameras
6. Record video stream
7. Send frames of video stream to responsible fog
8. At fog, Apply BC technology on the arrived T_s

9. Input: Transition (T_s) = spatial data frame; T = Timestamp; Nonce (n) = random number;
   Prev_Hash = hash of previous block;
10. While (T_s) *do*
11. Compute spatial block hash = SHA-256 hash function (T_s , T , Prev_Hash, n);
12. If computed Hash is authentic then
13. Add spatial block into the chain;
14. else
15. Drop the block;
16. n++ ;
17. end if
18. end while
19. return spatial blockchain;

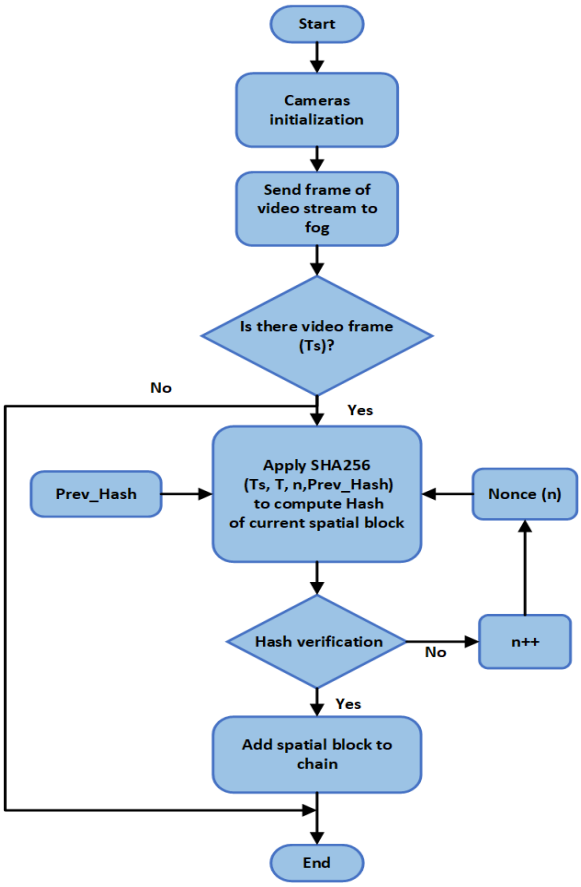

Figure 2 The flowchart of the fog based blockchain-IoST surveillance system

The proposed system's security depends upon the robustness of the blockchain technology, which is deployed within a decentralized network of fog nodes. This methodology reduces the risk associated with a single point of failure. Furthermore, the protection of data confidentiality on the blockchain is achieved by employing SHA-256 encryption to protect the metadata associated with each transaction.

By using the POW consensus protocol, commonly known as mining, transactions are encapsulated in a spatial block. It is highly secure and guarantees perfect operations in blockchain systems [20]. As depicted in *Figure 3*, a spatial blockchain is a linked chain of blocks that hold spatial data and connect them by a hash. It uses a crypto-spatial coordinate system utilizing SHA-256 to add immutable to the spatial blocks. SHA-256 algorithm encrypts the input plaintext to a hash, 256-bit binary, value [50]. Thus, demonstrating the inability of any participant to modify the stored data.

The first block in a blockchain network without a parent block is known as the genesis block. Each block contains data, such as the hash of the previous spatial block, The block's timestamp shows when it was created, the spatial data hash, and a numeric Nonce (32-bit or 8-hex-digits in our work) to guarantee that the proper hash is generated in a PoW method. The computed hash is subsequently compared to a specified difficulty hash as stated by the blockchain. If the resulting hash is equal to the difficulty hash, the transaction will undergo verification and afterwards, a new block will be appended to the blockchain. In the mining process, miners engage in the iterative adjustment of the nonce until they successfully discover a hash value that meets with the predetermined difficulty target hash.

3.3Experimental setup

The suggested video surveillance system for smart cities is implemented utilizing the iFogSim [51, 52] simulator, an IoT device toolkit, for two scenarios. iFogSim can simulate resource management and application scheduling strategies over edge and cloud resources in various scenarios and circumstances. Specifically, iFogSim facilitates the examination and evaluation of resource allocation strategies that are grounded in QoS metrics, such as latency, across various workloads characterized by factors such as tuple size and transmit rate [51].

In the first scenario, fog based blockchain-IoST deployment, fog nodes involve processing modules as shown in *Figure 4*. It simulates a physical topology consisting of a cloud, a proxy server, and two fog nodes. Each fog node covers one area with one actuator and four intelligent cameras, which are simulated as sensors, to record live video streams of the monitoring area. The configuration settings for the cloud server, proxy server, and fog nodes that are

considered throughout the experiment are shown in *Table 1*.

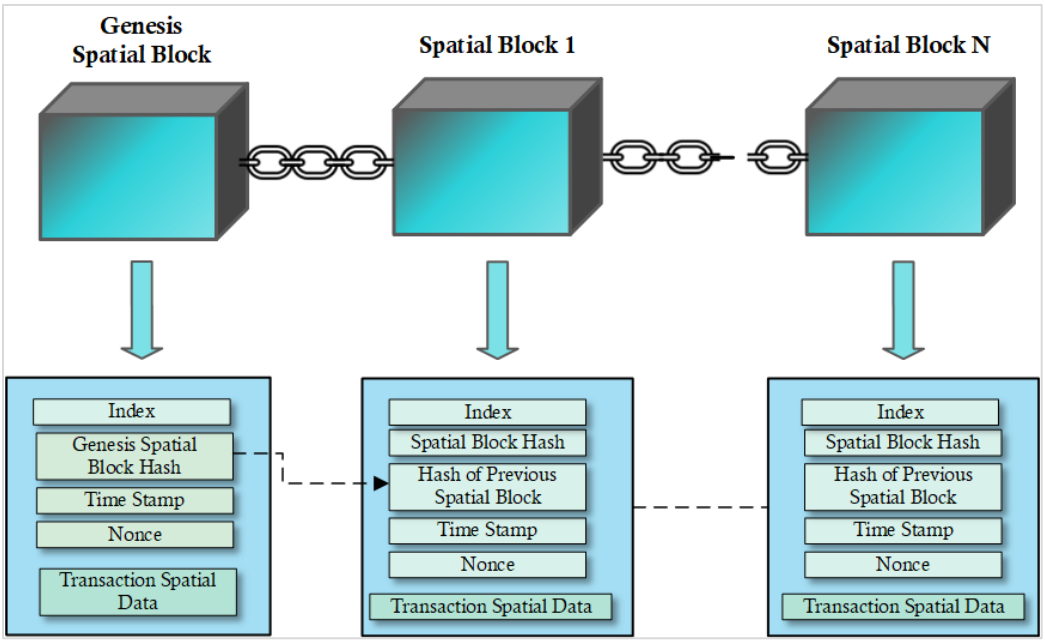

Figure 3 IoST- spatial blockchain structure

Where central processing unit (CPU), million instructions per second (MIPS), cost rate per million instructions per second used (RatePerMIPS), random access memory (RAM), uplink and downlink bandwidth configuration, busy power (node power consumption in a busy state), and idle power (node power consumption in an idle state). In the second scenario, cloud based blockchain-IoST deployment, all processing is done in the cloud as shown in *Figure 5* for simulating eight intelligent video cameras and an actuator that are all connected to the cloud through a proxy server. Cameras transmit the recorded video frames to the cloud directly via a proxy server. All the processes of the arrived spatial data are performed in the cloud server. Configuration parameters for the cloud server, and proxy server that were considered throughout the experiment are shown in *Table 2*.

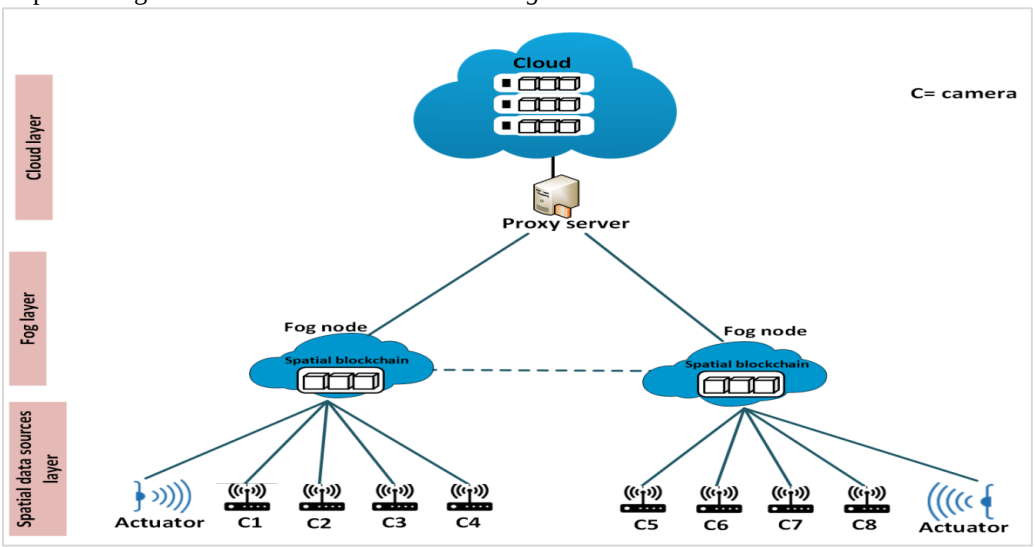

Figure 4 Fog-based architecture topology with eight cameras connected to two fog nodes and cloud server via proxy server

Table 1 Simulation Parameters of Fog Based Blockchain-IoST Deployment Model

Parameters	Cloud	Proxy	Fog
RAM (MB)	40000	4000	4000
CPU length (MIPS)	44800	2800	2800
RatePerMIPS	0.01	0.0	0.0
Uplink bandwidth (MB)	100	10000	10000
Downlink bandwidth (MB)	10000	10000	10000
Idle power (Watt)	16×83.25	83.4333	38.4333
Busy power (Watt)	16×103	107.339	107.339

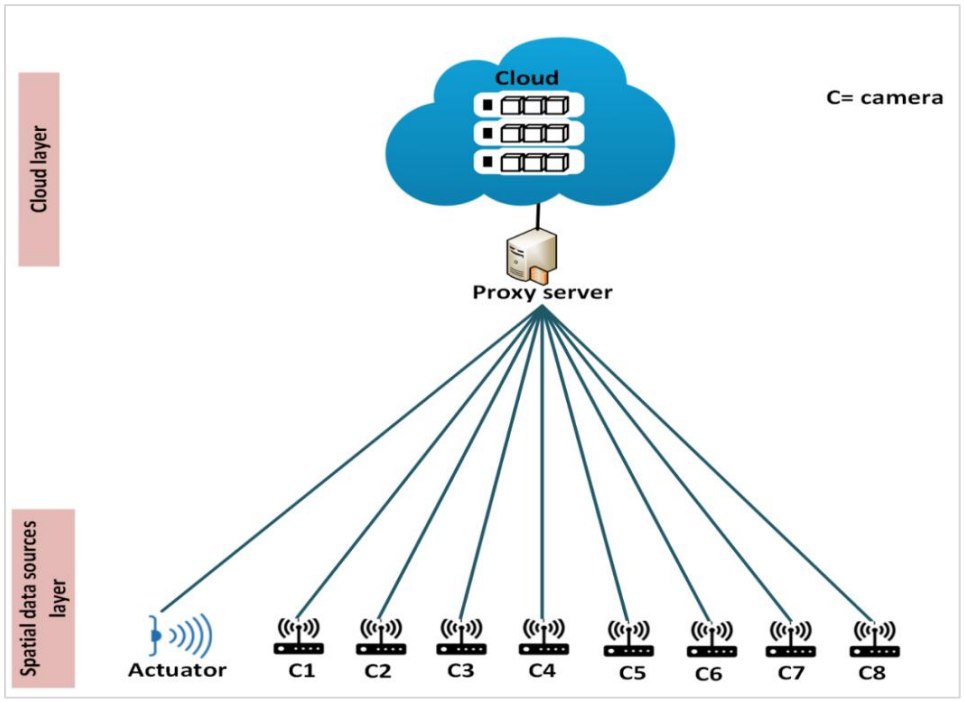

Figure 5 Cloud-based architecture topology with eight cameras connected to cloud server via proxy server

Table 2 Simulation Parameters of Cloud Based Blockchain-IoST Deployment Model

Parameters	Cloud	Proxy
RAM (MB)	40000	4000
CPU length (MIPS)	44800	2800
RatePerMIPS	0.01	0.0
RAM (MB)	40000	4000
Uplink bandwidth (MB)	100	10000
Downlink bandwidth (MB)	10000	10000
Idle power (Watt)	16*83.25	83.4333
Busy power (Watt)	16*103	107.339

4.Results and discussion

In this section the efficiency and scalability of the proposed surveillance system in fog based blockchain-IoST deployment are demonstrated and compared with the cloud based blockchain-IoST deployment for smart cities. The proposed system is evaluated using a variety of configurations and scenarios that consider network latency, usage, and energy consumption. The system's scalability is also evaluated by taking execution time and RAM usage into account in a variety of scenarios. The suggested system has a variety of surveillance areas that range from one to twelve, with four smart cameras per area.

4.1Network latency

The major advantage of fog based blockchain-IoST is that it avoids frequent cloud requests and conducts calculations at the network's edge, providing rapid response and reducing network latency. For efficient real-time applications, reducing network latency is

crucial to achieve PoW [10, 49]. The network latency for fog-based and cloud-based blockchain-IoST deployments is shown in *Figure 6* for a variety of scenarios including a range of camera counts. As a result of each fog node being particularly designed to handle spatial data for its area, it demonstrates a considerable reduction in latency for the fog-based paradigm. While with cloud based blockchain-IoST framework, a cloud server handles all the data processing, causing the latency to increase as the number of cameras ascends.

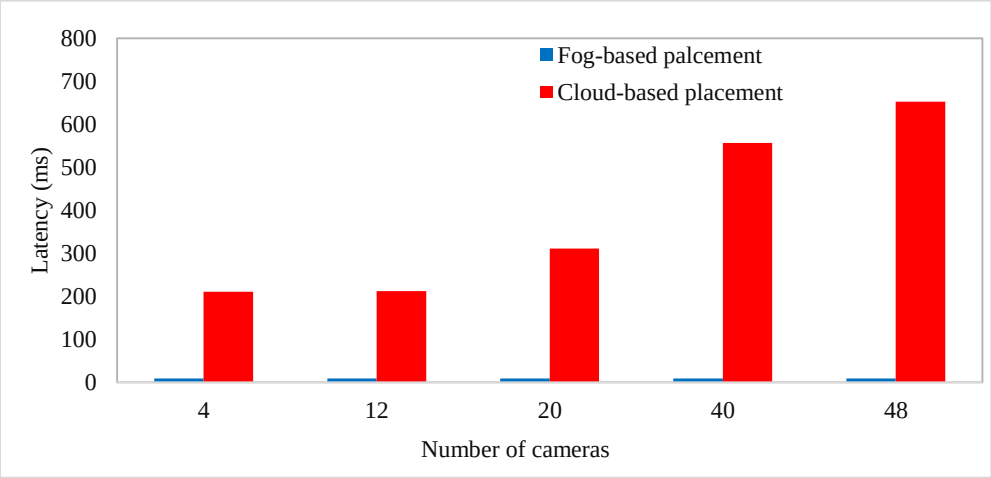

Figure 6 Comparison of fog based and cloud based blockchain-IoST in terms of latency

4.2Network usage

In the cloud-based model, network usage rises as all cameras are connected to the cloud server because all data is processed at one time on a single cloud server. Network usage arose as a result of increasing network traffic on the cloud server and reducing the network's data rates in cloud based blockchain-IoST. Fog computing is an effective approach for mitigating network traffic and facilitating scalability, making it particularly well-suited for IoST architectures. Therefore, network usage significantly dropped when fog based blockchain-IoST was considered, as seen in *Figure 7*.

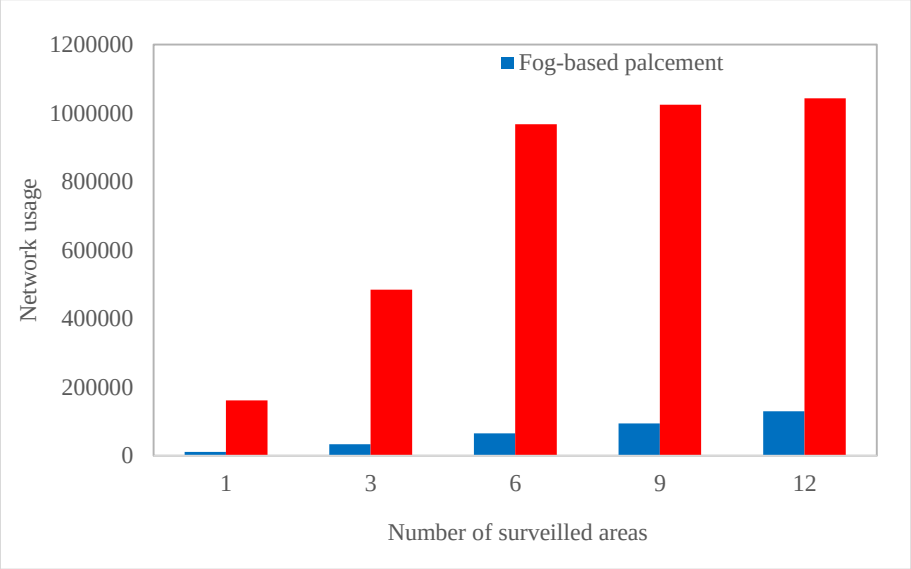

Figure 7 Comparison of fog based and cloud based blockchain-IoST in terms of network usage

4.3Energy consumption

To provide a general understanding of the amount of energy utilized by various components in the proposed system, the energy consumption of the devices in the two scenarios for the fog based and cloud based blockchain-IoST deployments is portrayed in *Figure 8*. *Figure 8* depicts a scenario with one cloud, one router, three fog nodes, and 12 intelligent cameras. When functions are deployed at fog nodes and without transmitting network data to the cloud, the amount of energy consumed in the cloud data center decreases. The study outcomes demonstrate that, for the same application, the video surveillance system in fog based blockchain-IoST produced a considerable reduction in energy consumption compared to processing in the cloud based blockchain-IoST deployments.

Complete list of abbreviations is shown in *Appendix I.*

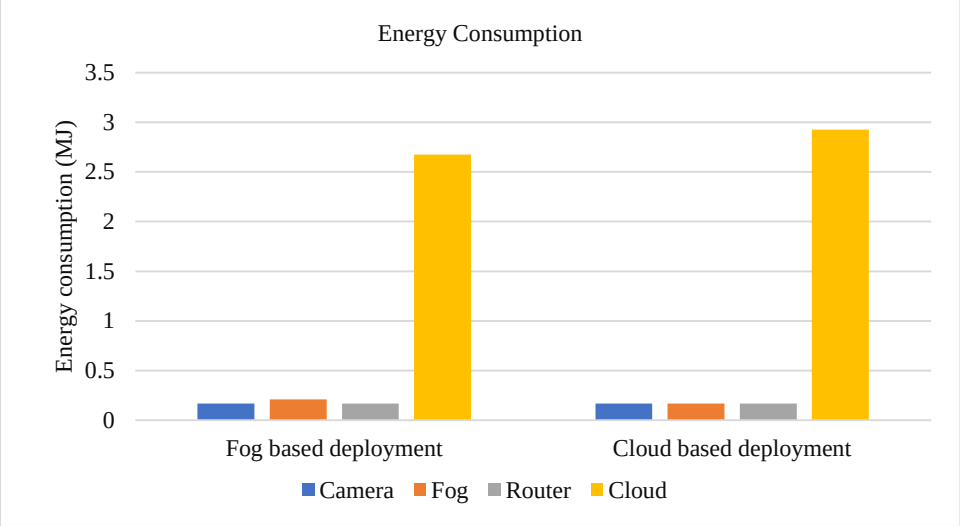

Figure 8 Comparison in fog based and cloud based blockchain-IoST in terms of energy consumption

4.4Limitations

Surveillance systems based on blockchain-IoST could assist smart cities by maintaining a secure, open, decentralized, and immutable record of all transactions generated by various sources, however, it possesses constraints. The first constraint is the capacity requirement. We propose the fog based blockchain-IoST to lighten the system. IoST-Chain spatial blocks are generated by a consensus algorithm that verifies the hash value of the previous block to assure data reliability. Only spatial data is embedded in the IoST-chain, so that the blockchain storage capacity does not exceed a particular amount. The second constraint is the consensus algorithm. PoW is utilized by the consensus algorithm for block generation, which necessitates an extensive amount of CPU operations and some network communication [42, 53].

5.Conclusion and future work

The primary objective of this study is to propose a hypothetical model of a futuristic video surveillance system by relying on the 5G and beyond 5G advanced technologies that incorporate IoST, edge computing, and blockchain. Therefore, a trustworthy video surveillance system is developed based on IoST for smart cities, with an emphasis on employing blockchain technology to accomplish the integrity and safety from manipulation of spatial data and appropriate for the safe storing of video data over a distributed ledger. The architecture of the fog based blockchain-IoST framework consisted of three layers: a cloud layer, a fog layer with fog nodes that each covered a region or area, and end devices, cameras and actuators. The proposed system has been evaluated in two configurations cloud-based and fog based blockchain-IoST using the iFogSim simulator. Concerning the metrics of network utilization, energy use, and application delay, the results of this work show the effectiveness of the fog-based IoST paradigm.

In the future, the suggested system can be subjected to additional evaluation under security threats like distributed denial-of-service (DDoS) attacks. Additionally, the effect of mobility on the system needs to be addressed. Moreover, it is recommended to incorporate geographic information system (GIS)

technologies, which enable efficient spatial data analysis and provide data visualization, into the proposed system.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

Author's contributions statement
Noor alsaedi: Conceptualization, Investigation, Data curation, Writing – original draft, Writing – review and editing. **Ali Sadeq Abdulhadi Jalal:** Analysis and interpretation of results, review, and supervision.

References
[1] Tekouabou SC, Cherif W, Silkan H. Improving parking availability prediction in smart cities with IoT and ensemble-based model. Journal of King Saud University-Computer and Information Sciences. 2022; 34(3):687-97.
[2] Gallo P, Nguyen UQ, Pongnumkul S, Barone G. Blockchain for smart cities: Applications for IoT and video surveillance systems. Innovations in Land, Water and energy for Vietnam's Sustainable Development. 2021:227-48.
[3] Jin Y, Qian Z, Yang W. UAV cluster-based video surveillance system optimization in heterogeneous communication of smart cities. IEEE Access. 2020; 8:55654-64.
[4] Ni J, Zhang K, Lin X, Shen X. Securing fog computing for internet of things applications: challenges and solutions. IEEE Communications Surveys & Tutorials. 2017; 20(1):601-28.
[5] Ghafir I, Prenosil V, Hammoudeh M, Baker T, Jabbar S, Khalid S, et al. Botdet: a system for real time botnet command and control traffic detection. IEEE Access. 2018; 6:38947-58.
[6] https://explodingtopics.com/blog/iot-trends. Accessed 18 September 2023.
[7] Kumar N, Jamwal P. Analysis of modern communication protocols for IoT applications. Karbala International Journal of Modern Science. 2021; 7(4):392-404.
[8] Al-Joboury IM, Al-Hemiary EH. Consensus algorithms based blockchain of things for distributed Healthcare. Iraqi Journal of Information and Communication Technology. 2020; 3(4):33-46.
[9] Deepak K, Badiger AN, Akshay J, Awomi KA, Deepak G, Kumar H. Blockchain-based management of video surveillance systems: a survey. In 6th international conference on advanced computing and communication systems 2020 (pp. 1256-8). IEEE.
[10] Awaisi KS, Abbas A, Zareei M, Khattak HA, Khan MU, Ali M, et al. Towards a fog enabled efficient car parking architecture. IEEE Access. 2019; 7:159100-11.
[11] Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. Sensors. 2019; 19(8):1-33.
[12] Baker T, Asim M, Samwini H, Shamim N, Alani MM, Buyya R. A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems. Computer Networks. 2022; 203:108676.
[13] Chen G, Xu B, Lu M, Chen NS. Exploring blockchain technology and its potential applications for education. Smart Learning Environments. 2018; 5(1):1-10.
[14] Boulos MN, Wilson JT, Clauson KA. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. International Journal of Health Geographics. 2018; 17:1-10.
[15] Chung WJ, Cho TH. A security scheme based on blockchain and a hybrid cryptosystem to reduce packet loss in IoV. International Journal of Advanced Technology and Engineering Exploration. 2021; 8(81):945-56.
[16] Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. ICT Express. 2020; 6(2):93-7.
[17] Ul Abadin Z, Syed M. A pattern for proof of work consensus algorithm in blockchain. In 26th European Conference on Pattern Languages of Programs 2021 (pp. 1-6).
[18] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review. 2008.
[19] Jamali J, Bahrami B, Heidari A, Allahverdizadeh P, Norouzi F. Towards the internet of things. Springer International Publishing; 2020.
[20] Sriman B, Ganesh Kumar S, Shamili P. Blockchain technology: consensus protocol proof of work and proof of stake. In the proceedings of intelligent computing and applications, Advances in Intelligent Systems and Computing 2021 (pp. 395-406). Springer Singapore.
[21] Barman N, Deepak GC, Martini MG. Blockchain for video streaming: Opportunities, challenges, and open issues. Computer. 2020; 53(7):45-56.
[22] Xu Z, Hu C, Mei L. Video structured description technology based intelligence analysis of surveillance videos for public security applications. Multimedia Tools and Applications. 2016; 75:12155-72.
[23] Chen N, Chen Y, Song S, Huang CT, Ye X. Smart urban surveillance using fog computing. In symposium on edge computing 2016 (pp. 95-96). IEEE.
[24] Memos VA, Psannis KE. UAV-based smart surveillance system over a wireless sensor network. IEEE Communications Standards Magazine. 2021; 5(4):68-73.
[25] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: a state of the art survey. Journal of Network and Computer Applications. 2020; 166:102693.

[26] Chaer A, Salah K, Lima C, Ray PP, Sheltami T. Blockchain for 5G: opportunities and challenges. In Globecom workshops 2019 (pp. 1-6). IEEE.
[27] Rago A, Ventrella P, Piro G, Boggia G, Dini P. Towards an optimal management of the 5G cloud-RAN through a spatio-temporal prediction of users' dynamics. In mediterranean communication and computer networking conference 2020 (pp. 1-4). IEEE.
[28] Rego A, Canovas A, Jiménez JM, Lloret J. An intelligent system for video surveillance in IoT environments. IEEE Access. 2018; 6:31580-98.
[29] Jeong Y, Hwang D, Kim KH. Blockchain-based management of video surveillance systems. In international conference on information networking 2019 (pp. 465-8). IEEE.
[30] Abdalla PA, Varol C. Testing IoT security: the case study of an IP camera. In 8th international symposium on digital forensics and security 2020 (pp. 1-5). IEEE.
[31] Fitwi A, Chen Y. Secure and privacy-preserving stored surveillance video sharing atop permissioned blockchain. In international conference on computer communications and networks 2021 (pp. 1-8). IEEE.
[32] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In symposium on security and privacy 2016 (pp. 839-58). IEEE.
[33] Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV. Efficient privacy preserving video surveillance. In 12th international conference on computer vision 2009 (pp. 1639-46). IEEE.
[34] Chen J, Ruan Y, Guo L, Lu H. BCVehis: a blockchain-based service prototype of vehicle history tracking for used-car trades in China. IEEE Access. 2020; 8:214842-51.
[35] Chen X, Xing Z, Karki B, Li Y, Chen Z. Blockchain simulation: a web application for it education. In 11th Annual computing and communication workshop and conference 2021 (pp. 0486-91). IEEE.
[36] Chukwu E, Garg L. A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. IEEE Access. 2020; 8:21196-214.
[37] Gallo P, Pongnumkul S, Nguyen UQ. BlockSee: blockchain for IoT video surveillance in smart cities. In international conference on environment and electrical engineering and industrial and commercial power systems Europe 2018 (pp. 1-6). IEEE.
[38] Khan PW, Byun YC, Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics. 2020; 9(3):1-21.
[39] Moolikagedara K, Nguyen M, Yan WQ, Li XJ. Video blockchain: a decentralized approach for secure and sustainable networks with distributed video footage from vehicle-mounted cameras in smart cities. Electronics. 2023; 12(17):1-11.
[40] Amofa S, Lin X, Xia Q, Xia H, Gao J. Blockchain-based health data sharing for continuous disease surveillance in smart environments. In 28th international conference on parallel and distributed systems 2023 (pp. 185-92). IEEE.
[41] Pane J, Verhamme KM, Shrum L, Rebollo I, Sturkenboom MC. Blockchain technology applications to postmarket surveillance of medical devices. Expert Review of Medical Devices. 2020; 17(10):1123-32.
[42] Na D, Park S. IoT-chain and monitoring-chain using multilevel blockchain for IoT security. Sensors. 2022; 22(21):8271.
[43] Lazaroiu C, Roscia M. Smart district through IoT and blockchain. In international conference on renewable energy research and applications 2017 (pp. 454-61). IEEE.
[44] Liu H, Tai W, Wang Y, Wang S. A blockchain-based spatial data trading framework. EURASIP Journal on Wireless Communications and Networking. 2022; 2022(1):71.
[45] Janarthanan S, Vijayalakshmi S, Savita, Ganesh Kumar T. Geospatial blockchain: promises, challenges, and scenarios in healthcare. Digitization of Healthcare Data Using Blockchain. 2022:25-47.
[46] Shirabe T. Classification of spatial properties for spatial allocation modeling. GeoInformatica. 2005; 9:269-87.
[47] Alsaedi N, Jalal AS. Big spatial data systems-a review. In 5th international conference on engineering technology and its applications 2022 (pp. 147-52). IEEE.
[48] Eldrandaly KA, Abdel-Basset M, Shawky LA. Internet of spatial things: a new reference model with insight analysis. IEEE Access. 2019; 7:19653-69.
[49] Li H, Xiezhang T, Yang C, Deng L, Yi P. Secure video surveillance framework in smart city. Sensors. 2021; 21(13):1-16.
[50] Sahib RH, Al-Shamery P, Salih E. An online e-voting system based on an adaptive ledger with singular value decomposition technique. Karbala International Journal of Modern Science. 2021; 7(4):1-22.
[51] Gupta H, Vahid Dastjerdi A, Ghosh SK, Buyya R. iFogSim: a toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience. 2017; 47(9):1275-96.
[52] Mahmud R, Pallewatta S, Goudarzi M, Buyya R. Ifogsim2: an extended ifogsim simulator for mobility, clustering, and microservice management in edge and fog computing environments. Journal of Systems and Software. 2022; 190:111351.
[53] Castro M, Liskov B. Practical byzantine fault tolerance. In OsDI 1999 (pp. 173-86).

Noor Alsaedi was born in Baghdad, Iraq, in 1983. She earned her B.Sc. degree in computer engineering from the University of Technology, Iraq, in 2006. Subsequently, she obtained her M.Sc. degree in wireless communication and network engineering from Universiti Putra Malaysia (UPM), Malaysia, in 2016. Presently, she is pursuing her Ph.D. in the Department of Information and Communication Engineering at the College of Information Engineering in Iraq. Her research interests encompass Network Security and the Internet of Things.
Email: nlight1124@gmail.com

Ali Sadeq Abdulhadi Jalal was born in 1958 in Baghdad, the capital city of the Republic of Iraq. He earned his bachelor's and master's degrees in Electrical and Communication Engineering at Al-Rasheed College for Engineering and Science, University of Technology, Baghdad, Iraq, in 1980 and 1986, respectively. Following this, he was appointed as an assistant lecturer in the field of Electronics and Communication Engineering at the same college. He achieved the positions of lecturer and assistant professor in 1994 and 2009, respectively. He completed his Ph.D. at the University Putra Malaysia (UPM) in 2013. Currently, he holds the position of Professor at Al-Nahrain University, College of Information Engineering. His primary research interests encompass Electronics, both Analog And Digital, as well as Antennas and Microwave devices.
Email: ali.jalal@nahrainuniv.edu.iq

Appendix I

S. No.	Abbreviation	Description
1	5G	Fifth Generation
2	AI	Artificial Intelligence
3	CCTV	Closed-Circuit Television
4	CPU	Central Processing Unit
5	DDoS	Distributed Denial-of-Service
6	DLT	Distributed Ledger Technology
7	DPoS	Delegated Proof of Stake
8	EE	Energy Efficiency
9	EH	Energy Harvesting
10	GIS	Geographic Information System
11	IP	Internet Protocol
12	IPFS	Inter Planetary File System
13	IoST	Internet of Spatial Things
14	IoT	Internet of Things
15	MIPS	Million Instructions Per Second
16	MITM	Man-In-The-Middle
17	ML	Machine Learning
18	PMS	PostMarket Surveillance
19	PoS	Proof of Stake
20	PoW	Proof of Work
21	PBFT	Practical Byzantine Fault Tolerance
22	QoE	Quality of Experience
23	QoS	Quality of Service
24	RAM	Random Access Memory
25	SDN	Software-Defined Networking
26	SHA	Secure Hash Algorithm
27	SoV	Site of View
28	TA	Trusted Authority
29	UAV	Unmanned Aerial Vehicles
30	VSD	Video Structural Description
31	WSN	Wireless Sensor Network