



Monitoring and surveillance systems based IoTs with Blockchain: Literature Review

Noor Ali Alshuraify¹ , Ali A. Yassin^{1,*} , Zaid Ameen Abduljabbar¹ , Vincent Omollo Nyangaresi^{2,3}

¹Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq.

²Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya.

³Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu 602105, India.

ARTICLE INFO

Received 22 April 2024
Revised 8 July 2024
Accepted 25 July 2024
Published 31 December 2024

Keywords :

Surveillance Systems, Real-time Monitoring, Blockchain, IoT.

Citation: N. A. Alshuraify et al., J. Basrah Res. (Sci.) 50(2), 42 (2024).
[DOI:https://doi.org/10.56714/bjrs.50.2.5](https://doi.org/10.56714/bjrs.50.2.5)

ABSTRACT

Globally, technology has developed in various sectors to improve individuals' quality of life and safety. Monitoring and surveillance systems are critical components of different industries' infrastructure. Monitoring and surveillance systems based on IoT have enhanced promptly in recent years, integrating with sophisticated technologies such as blockchain, deep learning, cloud computing, and edge computing. To the best of our knowledge, there are few reviews in the field of monitoring and surveillance-based blockchain. For that reason, we conducted a literature review to discuss different methods for addressing security and privacy problems in monitoring and surveillance systems based on IoT utilizing blockchain technology. Our research divides the papers into five sections which are surveillance systems, authentication mechanisms, artificial intelligence security mechanisms / Monitoring in different smart industries, and detection mechanisms. It also focuses on the use of blockchain technology and its types, the employment of external data storage that integrates with the blockchain for supporting its storage, and the type of tools used, to compare the previous studies. Additionally, the review research compares current methodologies in terms of shortcomings such as lack of security analysis, performance evaluation, malicious attacks, and data security during transmission. Our research introduces a comparison that includes security features such as mutual authentication, Anonymity, the employment of external storage, performance analysis. Also, the research gave a summary and analysis of previous work. Lastly, the study benefits beginner researchers in terms of saving time and effort.

*Corresponding author email : pgs.ali.yassin@uobasrah.edu.iq



1. Introduction

Information technology supports enterprises' digital transformation by integrating hardware, software, and networks seamlessly, allowing for more efficiency and creativity. Additionally, the enterprises' data security in the cloud is vital in defending against cyber-attacks, and providing secure and dependable access to the resources of industries from anywhere. One of the most important of these industries are oil and gas which they have contributed significantly to the national economy's growth and development during the last decades [1]. These industries are regarded as the world's most essential energy source, and its products power modern society by fueling vehicles for transportation and supply delivery. The fields of oil and gas are crucially imperative for practically every business because they are used in daily life [2]. As a part of oil and gas fields, Millions of kilometers of pipelines are positioned across the world to transmit vast amounts of fresh water, fuels, crude oil, and natural gas. Most oil-producing countries see these pipelines as energetic to their national economies [3]. It is known that pipelines are located in isolated and remote areas. Because pipelines cross great distances, tunnels, hills, and canals, they are frequently subjected to serious security risks such as pollution, leakage loss, terrorism, and theft of pipeline contents [3]. Besides, long-term use of oil pipelines can cause cracks and leaks owing to aging, environmental influence, and man-made damage. Furthermore, the oil delivered by pipeline is combustible and explosive. Therefore, leakage can lead to explosions and accidents, resulting in significant economic losses and environmental degradation. It also hinders production and raises the likelihood of pipeline catastrophes [4].

Based on the aforementioned problems, surveillance systems are employed to overcome them. Essentially, video surveillance equipment is installed at a predetermined distance to allow the watched items to be tracked. These locations are frequently outfitted with thousands of video surveillance devices [5]. Surveillance technologies have grown increasingly prevalent in monitoring the physical surroundings in diverse environments [6]. Intelligent video surveillance systems monitor suspicious activity and issue alarms without human interaction [7]. Where it provides intelligence to monitoring equipment, allowing it to process and read data in real-time, analyze monitoring scenes, and accomplish checks besides performing video capture, transmission, storage, playback, and watching [5]. Moreover, when an anomaly behavior is detected in the monitoring scenario, a prompt message is automatically sent to the monitoring system for taking appropriate measures to notify the monitoring personnel to intervene manually, thereby improving the security system's intelligence level [8].

Although the above-mentioned characteristics, surveillance devices create significant privacy and security issues since they are more susceptible to attacks [9]. Where, attackers may manipulate the visual content of surveillance system footage locally or remotely, leaving them susceptible [10]. For example, the Mirai botnet infected hundreds of thousands of cameras and launched a DDoS attack on key infrastructure [9]. It is worth noting that some surveillance systems are centralized data storage, which exposes them to challenges of trust, validity, and integrity of the information. This underlines the importance of having a technical solution that can verify the integrity of video surveillance data transmitted across systems controlled by different confidence levels [11].

The blockchain technology and its distinctive characteristics aim to introduce an ideal solution for addressing the aforementioned issues and obstacles [12]. The blockchain technique consists of a sequence of blocks that are cryptographically produced and linked together, with hash values connecting them sequentially. Blockchain technology's high-security level is derived from integrated technologies such as asymmetric encryption algorithms, hash algorithms, Merkle hash tree, consensus algorithms, and smart contracts [13]. Therefore, blockchain technology offers unique benefits over other traditional systems. Furthermore, a decentralized system can be used to address the most prevalent issues related to a centralized design. In addition, blockchain features taking part in providing a trusted system that can efficiently struggle with many types of cybersecurity attacks [14]. Likewise, blockchain technology ensures system stability in the event of an attack or node downtime. As a final result, blockchain outperforms traditional systems in terms of performance, external attack resistance, and fault tolerance [15].

To the best of our knowledge, there are many reviews of surveillance systems, and numerous reviews of blockchain and its applications, but there are almost few reviews in the context of

monitoring and surveillance systems based IoT with blockchain. For that reason, in this paper, we conducted a review that integrates monitoring and surveillance systems based IoT with blockchain technology and discuss the challenges that previous studies face. Additionally, we make a comparison between the systems according to their method, tools that are utilized such as encryption algorithms, programming languages, and the types of blockchain. Moreover, Our research makes a comparison that includes security features such as mutual authentication, Anonymity, the employing of external storage, performance analysis that comprises the computation and communication costs, and attacks that the research papers neglected to address. Fig 1 illustrates monitoring and surveillance systems.

We make several contributions in the realm of monitoring and surveillance systems based on IoT with blockchain technology:

- ❖ Our research introduces five sections which are surveillance systems, authentication mechanisms, artificial intelligence, security mechanisms / Monitoring in different smart industries, and detection mechanisms, where every section seeks the advantages and disadvantages of each method.
- ❖ Also, we conducted a study that included comparisons that rely on the security aspect in terms of the types of blockchain used and the tools utilized such as languages, encryption methods, and artificial intelligence algorithms, as well as the methodology used.
- ❖ The study identifies several security flaws in present systems, including a lack of detailed security analysis, scalability challenges, storage constraints, a lack of performance evaluations, and data security issues during transmission.
- ❖ Analyzes the proposed schemes that integrate monitoring and surveillance systems based IoT that utilize technologies such as blockchain and artificial intelligence to verify data integrity, identify fraud, facial recognition, and store data securely.
- ❖ Discuss the applications of monitoring and surveillance systems based IoT in a variety of industries, including healthcare, agriculture, oil and gas, and smart industries, demonstrating their adaptability and relevance.
- ❖ This study will help beginner researchers in monitoring and surveillance systems based on IoT in different sectors, particularly in the oil and gas industry, by clarifying the primitive tools and recommending the best type of blockchain to use. This will save time and effort during research.

The rest of the paper section 2 elaborates on primitive tools, section 3 describes the related work. We conclude our paper in section 4.

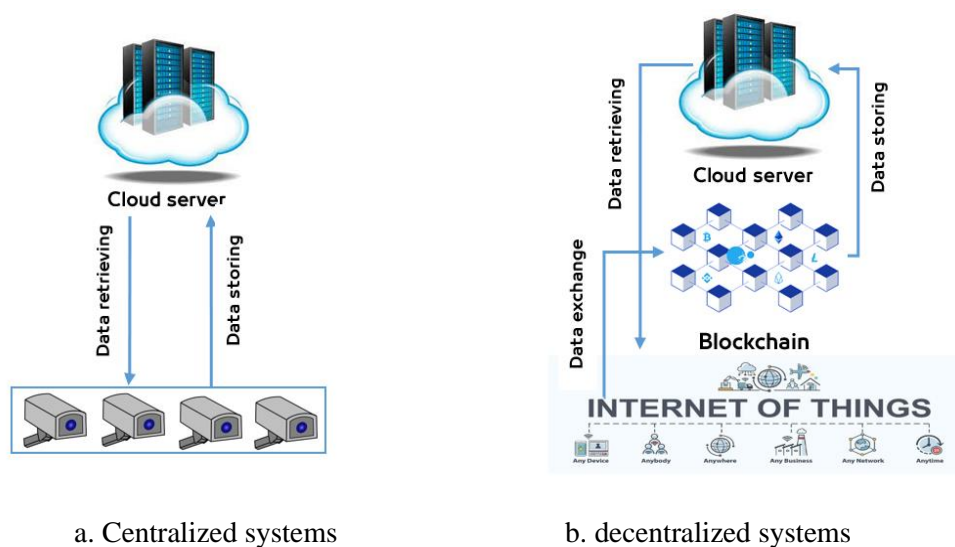


Fig.1. Illustrates monitoring and surveillance systems

2. Primitive Tools:

2.1. Secure Hash Algorithm-256 (SHA256):

The National Security Agency (NSA) considers a variant of the SHA-256 algorithm. Furthermore, SHA-256 is used by prominent encryption protocols such as SSL, TLS, and SSH, as well as open-source operating systems such as Unix/Linux [16]. Moreover, it is a one-way hash function that compresses variable message lengths into fixed-length code; it is employed for its differentiating characteristics, such as fixed-length output and the impossibility of accessing the original content. As an outcome, it is a potent instrument for achieving security objectives [17],[18]. Since the original data is difficult to obtain, deciphering the hash value is almost impossible and the sheer number of viable possibilities makes the brute force method impractical; Therefore, it is very difficult to find two data items that have the same hash (known as a collision), and in addition, the result is permanently 256 bits regardless of the text size [16].

Blockchain uses it in addition since it improves resistance to collision attacks and makes integrating and collaborating with pre-existing tools, libraries, and infrastructure easier. Furthermore, it delivers a high degree of security while maintaining computational efficiency, which is critical for blockchain network performance. This strikes a solid compromise between security and efficiency[17],[18].

2.2. Elliptic Curve Digital Signature Algorithm (ECDSA):

Scott Vanstone introduced ECDSA in 1992 [19]. The elliptical curve digital signature algorithm (ECDSA) employs ECC to establish a digital signature of data, ensuring its authenticity without affecting performance, reducing packet size and transmission overhead improving security performance, ECDSA's 160-bit key minimizes communication overhead and promoting privacy [20]. See Fig. 2.

The NIST Cryptographic Algorithm Validation Program has authorized and certified the use of ECDSA for industrial applications due to its low complexity and minimal storage. ECDSA enhances computational performance and maintains a suitable degree of robustness to offer high-performance asymmetric cryptography techniques [14].

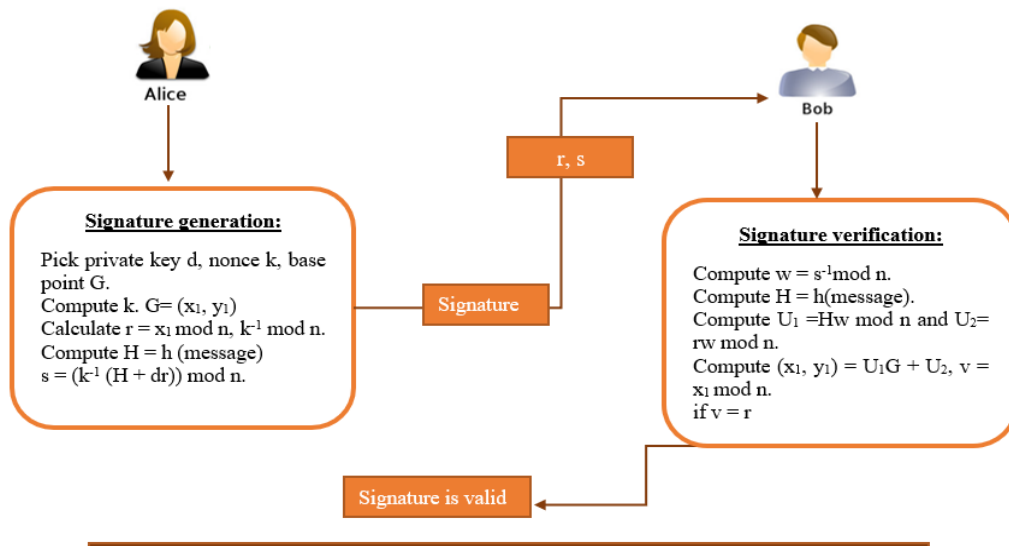


Fig. 2. Illustrates Elliptic Curve Digital Signature Algorithm

2.3. InterPlanetary File System (IPFS):

IPFS is a mechanism for storing data in distributed locations. Each file that is kept on IPFS has a unique hash that is assigned to it. Its deduplication process is effective and it is not restricted by a central server. In addition, information uploaded to the system may be deposited indefinitely [21]. The peer-to-peer communication network allows devices to store and share data in a distributed file system. IPFS outperforms blockchain and cloud storage by five times and 21 percent, respectively [13]. It uses a point-to-point storage technique for its protocol storage, which helps it meet this requirement. From a security standpoint, IPFS uses the hash function SHA-2 (SHA2-256) and has a large address space of 2^{256} , making it difficult for hackers to divulge [13].

Some researchers incorporate blockchain with IPFS as third-party storage due to its unique and valuable features [13]. Besides, high-capacity storage, high concurrent access, a safe content-addressed block storage paradigm, and high throughput [21]. See Fig. 3.

2.4. Scyther Tool:

A tool for assessing a scheme's security and weaknesses. The tool's operation is explained in two phases. This tool provides a formal evaluation of security protocols and allows for fast investigation of their properties. Used to assess the security and deficiencies of schemes. In order to verify protocol soundness, Scyther is guaranteed to complete in the first step and to allow an infinite number of sessions. Making the proof tree is an option. Scyther, the second stage, provides attack behavior types to facilitate graphical user interface analysis. Proposed schemes should be stated using the security protocol description language (SPDL), which describes protocols and schemes and allows for encryption, decryption, and signatures. These important cryptographic operations are utilized in message sending and receiving between components, as well as their respective purposes. The proposed scheme is written using SPDL language and the results are presented in the cases of automatic claims and verification claims [22], [23]. Fig 4 demonstrates Scyther tool GUI and parameters.

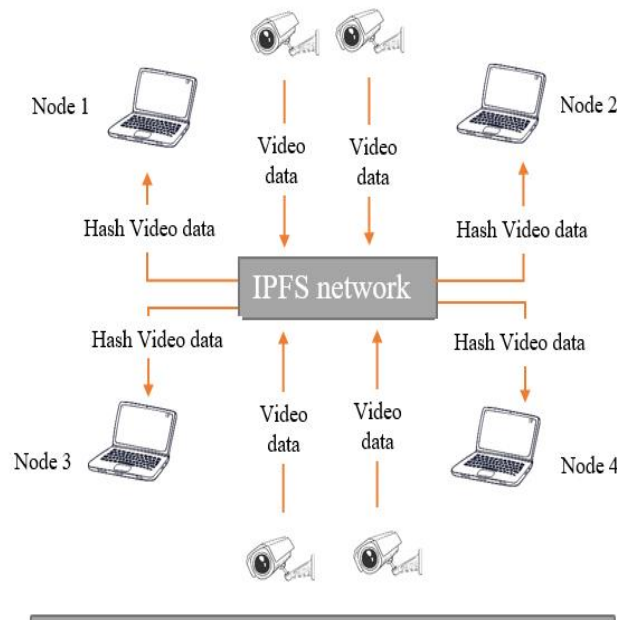


Fig. 3. Illustrates surveillance devices with IPFS-based blockchain

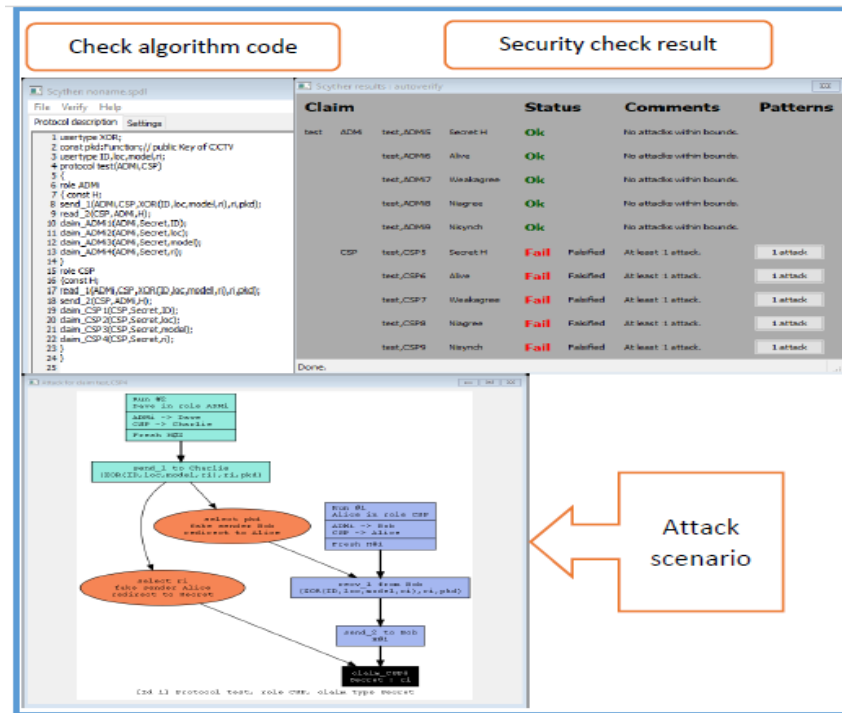


Fig. 4. Illustrates Scyther tool GUI and parameters.

2.5. AVISBA Tool:

It is applicable to all technologies and may analyze and research any methodology. It is a widely acknowledged and reliable software tool for automatically authenticating (depending on the push-button approach) the security features of protocols used in server-client interactions and the Internet of Things [24]. This protocol was implemented in HPSL; when the protocol was developed, an HPSL2IF translator turned the code into an intermediate format (IF)[25].

2.6. Blockchain programming tools:

2.6.1. Ganache:

A local development blockchain simulates the operations of a public blockchain and is used to release smart contracts and test them. Ganache enables ten accounts with 100 Ether to test smart contracts locally on the blockchain [26].

2.6.2. Truffle:

A powerful tool for Ethereum smart contracts. Truffle is a command-line application with an integrated smart contract compiler. In addition to being used for the compilation, distribution, and linking of smart contracts, it also functions as a platform for testing automated contracts and manages networks and packages. It develops smart contracts using the Solidity programming language [27].

2.6.3. Solidity:

A contract-oriented, high-level programming language that can be used to construct smart contracts. The high-level, statically typed programming language is Turing-complete. It is designed to target the EVM and was inspired by C++, Python, and JavaScript. Solidity is statically typed and supports libraries, inheritance, and advanced user-defined types and allows the construction of contracts for a variety of reasons, including crowdsourcing, voting, multi-signature wallets, blind auctions, and more [28].

2.6.4. Python:

A popular high-level programming language that serves several purposes. The design philosophy prioritizes code readability, and the syntax enables programmers to express concepts with fewer lines of code. The language elements let users design unambiguous programs on both small and large scales. Python supports several programming paradigms, such as object-oriented, imperative, functional, and procedural approaches. Also, it offers dynamic typing, automated memory management, and a robust standard library. In addition, interpreters are available across several operating systems [29].

3. Relate work:

The security and integrity of monitoring and surveillance systems based IoT have been a hot topic for researchers since the evaluation of the industrial sector [30]. We reviewed research articles that focus on surveillance systems, authentication mechanisms, artificial intelligence, security mechanisms/monitoring in different smart industries, and detection mechanisms. Table 1 and Table 2 clarify the comparison between research papers. Table 3 illustrates the analysis of the previous studies' sections.

1. Surveillance Systems

Nagothu et al. 2018 [31] proposed a microservice architecture for scalable, maintainable, and secure smart surveillance systems. Surveillance operations, including object identification, tracking, and feature extraction, were built as cooperative microservices that run independently within separate processes. It offered a versatile, testable, and maintainable platform for development and deployment. Blockchain and smart contracts introduced decentralized security to secure and synchronize data across communication channels. Smart contracts enabled the enforcement of data access rights.

This paper did not specify how the proposed system would work with current surveillance systems or infrastructure. This might be difficult if the system needs to communicate with legacy systems or devices that do not support the microservices design and blockchain technology.

Although the scalability and flexibility of the microservices architecture and blockchain technology it presents. However, it did not provide an analysis of the performance in terms of computation and communication costs.

Michael Kerr et al. 2018 [32] demonstrated a functioning implementation of distributed ledger technology for categorizing evidence video of CCTV. In addition, this paper presented a real-time blockchain camera prototype, as well as a system for managing and coordinating its use and distribution. This application was particularly useful for law enforcement organizations handling large amounts of CCTV evidence. Also, it explored scalability and applicability through simulations and real-world experiments. Besides, the article illustrated the integration of blockchain technology and an innovative digital watermarking application can address the challenge of protecting trustworthy evidence in scattered networks.

Although blockchain storage has challenges and at the same time CCTV cameras transmit large amounts of CCTV video evidence, the proposed scheme did not utilize an external data storage which leads to redundancy of video data and congestion on the network.

Rong Wang et al. 2019 [5] produced a system consisting of video surveillance, edge computing, permissioned blockchain, CNNs, and IPFS technologies. Permissioned blockchain is characterized by non-tampering, security encryption, and fault tolerance ensuring the system's resilience and stability. The large-scale wireless sensor's information collecting and data processing were accomplished by integrating an edge computing network and computation. The huge video data storage was achieved by utilizing the IPFS storage service. Also, CNNs were utilized to provide real-time monitoring.

The paper did not provide a security analysis of privacy breaches during video data transmission. Moreover, it did not present performance analysis in terms of compression ratio calculation for IPFS storage.

Michelin et al. 2020 [11] offered a method for verifying the data integrity of collected surveillance camera data by utilizing lightweight blockchain technology. The design had a three-layer architecture, with trusted surveillance cameras deployed in the sensing layer, trusted gateways in the transportation layer that handles video streaming and blockchain maintenance, and a third-party storage layer that stores surveillance videos using the Interplanetary File System Network (IPFS).

Uda 2020 [33] proposed a method for recognizing infractions and unlawful behaviors captured on surveillance cameras, as well as preventing video record forgeries. To ensure integrity, the system signed and chained message digests of video recordings using blockchain.

Khan et al. 2020 [34] provided a proposed solution that protects the validity and integrity of security camera records by preserving the CCTV footage's information on Hyperledger Fabric, which is a private blockchain platform. The system encrypted the image sensor's video and information, then forms a block, which is accepted. The proposed system also included user and device registration, with each peer receiving a unique key. Only approved devices and users could access the system.

Hence, Michelin et al. 2020 [11], Uda 2020 [33], and Khan et al. 2020 [34], What flawed them was that they neglected to provide a security analysis and did not describe the sorts of conceivable attacks, such as dictionary, impersonation, and Sybil that the proposed solutions could defend against. They also ignored discussing communication and computation expenses. Furthermore, they send all video data to be stored, which causes storage concerns.

Fitwi et al. 2021 [30] the paper described the development of SePriS, a privacy-aware smart surveillance system that uses blockchain technology and smart contracts to overcome difficulties with distributed access to surveillance videos. The system was made up of off-BC distributed video storage locations, BC nodes linked to Smart Access Controllers (SACs), and users with various access levels. Access to surveillance footage was provided using fine-grained access control restrictions established in smart contracts, and all video access actions were registered and kept on the blockchain. The proposed method used cryptographic techniques such as elliptic curve public encryption/decryption, a DCT-AES-BS mechanism, and digital signatures to transmit messages and video frames securely and privately. A Permissioned Blockchain (PBC)-based system was presented for the safe sharing of recorded surveillance movies among various SACs and authorized users, allowing secure and privacy-aware access to surveillance recordings kept on distributed off-BC sites. The proposed scheme provides anonymity in a partial way which may pose several attacks such as Sybil.

Tahir et al. 2021[35] developed a secure exchange of encrypted CCTV recordings used as evidence in court proceedings for legal purposes. To safeguard privacy in movies, the Gaussian Mixture Model (GMM) detected foreground motion before applying reversible eXclusive-OR (XOR) encryption to the observed information. Hyperledger Fabric was used to handle a legitimate chain of evidence using permissioned blockchain technology.

The paper's scope was constrained, since it concentrated on a specific situation of CCTV video evidence handling for remote court services, which may limit its application to other contexts. Furthermore, this work made no mention of video compression, which is an important technique for reducing storage while preserving quality. Also, it abandoned discussing attacks addressing.

Lee et al. 2021 [36] suggested a secure Merkle tree using a blockchain-based multimedia intelligent video surveillance system that protects privacy. The goal of the article was to use blockchain technology to address security and privacy issues in cloud-based intelligent surveillance systems. The suggested method utilized the technology of blockchain to guarantee the security and integrity of the cloud-based CCTV system.

What flawed this scheme was suffered from a lack of security analysis, which is important to detect the resilience and weaknesses of the proposed system against various attacks. Moreover, the performance evaluation of the suggested scheme was not included for measuring its applicability and effectiveness in the real-world distribution of CCTV systems.

The proposed scheme of Zhang et al. [37] In 2024, included a blockchain-based aberrant data storage model for cereal and oil video monitoring to assure traceability, security, and robustness of anti-tamper. The system used a dual-storage model dependent on blockchain and InterPlanetary File System (IPFS) to ensure data security while also relieving the storage burden on the blockchain.

Furthermore, it investigated the YOLOv7-based target recognition technique, as well as designed and implemented an anomaly detection model for grain depot video surveillance data. Then it extracted and saved frames with anomalous behaviors in videos to rapidly generate a summary while decreasing data redundancy.

Despite the good characteristics the method presented, but there is a challenge in the storing process of this scheme, where it relied on saving all original video data on IPFS without encrypting them which led to potential attacks such as MITM, Replay, and Sniffing.

2. Authentication mechanisms

In 2018, the paper of Hammi et al. [38] suggested bubbles of trust, a unique decentralized method that guarantees reliable device identification and verification. It further safeguarded the availability and integrity of the data. Extremely, this method, which established safe virtual spaces (bubbles) where objects could recognize and trust one another, was dependent on the security benefits offered by blockchains. It additionally comprised an actual Ethereum blockchain and C++ language implementation of the mechanism. Finally, the outcomes demonstrated its affordability, effectiveness, and capacity to meet IoT security standards.

What defected this paper that it overlooked to mention the type of consensus protocol. According to its utilization of the Ethereum blockchain, it might suffer from high costs due to the existence of the miners who validate the transactions exchange fees.

This research Lin et al. 2020 [39] developed a unique safe mutual authentication method that may be used in various applications, such as smart homes. In particular, the suggested method combined message authentication code, group signature, and blockchain to offer dependable auditing of users' access histories, anonymous group member authentication, and effective home gateway authentication, respectively. Additionally, an implementation and assessment to show the system's viability demonstrated that it fulfilled the security and privacy criteria, including traceability, anonymity, and confidentiality.

This paper is characterized by good categories such as security and performance analysis, but despite that, it omitted to utilize external data storage, especially since there is an amount of data transferred between components and as known the blockchain has limited storage to store this big data.

Yang et al. 2021 [40] proposed a blockchain-based authentication technique that is both safe and lightweight for IoT systems. The modular square root (MSR) technique ensured authentication security and efficiency, while blockchain enhanced security and scalability. The smart contract mechanism guaranteed that only registered devices or users could access the services they subscribe to.

This work did not cover the use of third-party storage for data since these devices transmit big data and the blockchain's storage capacity is limited, and it did not discuss the security of data during the transfer process from devices before storing operation on the blockchain or server, nor the methods that used to prevent attacks from messing with it during the transmission.

Vivekanandan et al. 2021 [41] suggested a blockchain-based authentication mechanism to ensure the uniqueness and security of IoT device communication in 5G-enabled smart city applications. The proposed method registered IoT devices on a private blockchain, which also includes a Distributed Ledger (DL) for storing information about IoT credentials.

This paper does not specifically discuss mechanisms to prevent data manipulation by attackers such as Sniffing and Eavesdropping at the device level before it is stored in the blockchain or server.

Yu et al. 2023 [42] introduced a blockchain-based authentication and authorization solution for distributed mobile cloud computing services. It used smart contracts to dynamically modify access privileges and includes an additional authorization mechanism.

This effort suffers from sending plaintext transactions stored on the transparent blockchain, where the user's registration information is publicly available, which may result in a breach of privacy. Meanwhile, it did not address possible threats such as sniffing, Sybil, 51% attacks, or the use of third-party storage.

In 2023, the method of Hwaitat et al. [43] presented a novel strategy for a large-scale Internet of Things system built on a permissions-based blockchain that offered users a lightweight authentication system and optimized data storage. Besides, most applications that rely on blockchain technology

had been solved by the suggested approach, which notably helps with scalability and optimum storage. As well, this method used homomorphic encryption for the first time to encrypt IoT data at the user's end and upload this data to the cloud. Based on comprehensive simulation findings, the suggested approach was contrasted with alternative benchmark frameworks. Additionally, the research contributed by developing a unique Internet of Things strategy built on a trust-aware security method that connects exceptional IoT services while enhancing security and privacy.

What faced this paper was probably a delay in data retrieval due to uploading the IoT-encrypted data to the cloud, especially when data needed to be retrieved from the cloud for integrity test.

Chen et al. 2024 [77] proposed an enhanced blockchain-based method for IoT that prioritizes anonymous authentication and safe data transfer. This approach tries to anonymously authenticate IoT devices while simultaneously ensuring secure data delivery. Furthermore, it is intended to withstand security concerns such as impersonation, man-in-the-middle, and denial-of-service attacks while lowering computational and communication costs.

The IoT device, which is well-known for transmitting large volumes of data on a regular basis, may face issues in terms of unnecessary and repeated data, resulting in a system overload.

3. Artificial intelligence

R. Vamshidhar Reddy et al. 2020 [44] involved improving security for extracted facial expressions and body motions using Blockchain technology stored in BigchainDB. The technology concentrated on reducing the susceptibility of extracted facial expressions and body motions to modification by hostile actors. The extracted characteristics were kept securely and tamper-resistant using Blockchain Technology, especially BigchainDB. This technique protected the integrity and confidentiality of the data about facial expressions and body motions gathered from surveillance footage.

The paper did not discuss how to protect the privacy of individuals whose data is being captured and extracted, especially if the data is not anonymized or encrypted before the storing process or during transmission.

Jain et al. 2022 [45] presented a method for securely and impenetrably storing and managing data via a distributed ledger. Furthermore, their suggested system employed artificial intelligence to evaluate data and make decisions depending on the information collected by sensors. It also utilized biosensors to collect medical information from patients in real-time. Additionally, it also used a microservices design to facilitate scalability and avoid duplication of effort.

The defect in this paper is that did not discuss the registration process of users or patients, nor debate security analysis or the ability to overcome attacks such as impersonation and dictionary.

The paper research of Selvarajan et al. [46] in 2023 included techniques for privacy preservation, attack detection, and trust management. The project's goal was to design (AILBSM) mechanism, which was an AI-based Lightweight Blockchain Security Model. Additionally, it was designed to safeguard the security and privacy of IIoT systems, It comprised three layers of security processes: first, trust evaluation to ensure data authentication, the IIoT sensor device's trustworthiness, attack prevention utilizing a lightweight blockchain system, and attack categorization via an AI mechanism. Second, trust verification checked data supplied by IIoT sensor devices to determine if a machine has been misdirected or tampered with. It further employed a lightweight consensus Proof-of-Work (LCPoW) protocol to protect the anonymity of IIoT systems. Then, it performed data authentication to safeguard the IIoT system from potential attacks or intrusion. Furthermore, an Authentic Intrinsic Analysis (AIA) approach was applied to mitigate cyber-attack effects by transforming the characteristics into encoded data. Lastly, it adopted the Convivial Optimized Sprinter Neural Network (COSNN) algorithm to categorize normal and invader data accurately based on input data from the privacy preservation module.

Although the features above, the paper does not come up with details on the proposed scheme security analysis, which is crucial to prove the validation of the system's security and its triumph over cyber-attacks.

In 2024, the work of Ghani et al. [47] conducted a research included the development of a decentralized facial recognition system (DFRS) based on blockchain technology to offer strong data

security and extremely accurate face recognition capacity. It stressed the application of privacy computing, namely generative adversarial networks (GANs) alongside blockchain technology. This novel solution required segmenting face traits into multiple clusters, each regulated by a specific node and enabled by smart contracts in order to protect interactions and privacy. The suggested privacy protection measures were in response to the growing volume of face data and addressed the crucial need for decentralized safe facial data management. Furthermore, the study presented a multi-tiered security architecture with distinct security protocols for each level to improve access management and the integrity of data. Employing sophisticated deep learning architectures increased security by offering the greatest protection for data kept on a blockchain, ensuring facial recognition accuracy, and raising security requirements.

What flawed this paper, that it omitted to utilize external data storage and did not provide a security analysis about the way that the proposed scheme addressed the attacks.

Hennebelle et al. 2024 [48] proposed an end-to-end automated IoT-edge-AI-blockchain system for diabetes prediction using risk variables. The solution used edge computing to modify risk factor data acquired from IoT devices before sending the preprocessed data to the blockchain. The blockchain maintained patient medical information, machine learning model parameters, and prediction results in a distributed and replicated ledger, assuring user data confidentiality and privacy. The solution employed a multi-ledger permissioned blockchain architecture to allow variable access control rights and to enable the creation of a separate ledger for cooperating allied health professionals. The system was made up of transactions, events, participants, and assets, and blockchain was used in an AI-based prognosis/diagnosis assistance system for healthcare management.

The study stressed the proposed system's security and privacy features; however, it did not give a detailed analysis of potential security risks that might arise during the implementation of the proposed scheme. Besides, the paper did not present the registration process of patients and medical experts in detail.

Mahalingam et al. 2024 [49] included the construction of a novel blockchain-based cryptosystem dubbed RNECB for safeguarding IoT-sensed agricultural field data. The system used Recurrent Neural Networks (RNN), Elliptic Cryptosystems (ECC), and blockchain technology to improve security, data privacy, and transparency in IoT-based intelligent agriculture systems. The RNECB model was designed to predict crop yields, identify pests and diseases, monitor weather trends, enable secure communication between IoT devices, construct a tamper-proof ledger of agricultural data, and enhance supply chain management in agriculture. The suggested method aimed to improve security, transparency, and data privacy in IoT-based agricultural monitoring systems.

This paper did not work in a phases way, where it omitted to discuss the setup phase which is an important component in the system, and not obvious who is responsible for creating and distributing encryption/decryption keys over the network [50].

4. Security mechanisms / Monitoring in different smart industries

Choi et al. 2020 [51] constructed a private blockchain for the Nuclear Power Plants (NPP) environment and proposed a novel system to monitor the data integrity of Programmable Logic Controllers (PLCs) using this blockchain. Real-time monitoring of PLC integrity (every 5000-6000ms) could protect against cyber-attacks. The blockchain system was used to monitor the integrity of an NPP's RPS (the Reactor Protection System), or safety system. The Areal RPS prototype was utilized to create the monitoring system, and its validity was tested experimentally. This study was the first to combine blockchain with PLCs for security monitoring.

The suggested system's scalability is not covered in the study. Since blockchain has limited storage, it is unknown how the system will function while managing an enormous number of transactions or when the number of nodes in the network rises.

Khan et al. 2020 [52] introduced a permissioned private blockchain-based system to safeguard and encrypt images. In the system, an image's cryptographic pixel values were saved on the blockchain, assuring the privacy and safety of the data. Besides, the paper examined the strength of suggested image encryption algorithms against different attacks using the number of pixels change rate (NPCR), information entropy analysis, and the unified averaged changed intensity (UACI). Moreover, the scheme's entropy values were close to the ideal of 8, making it resistant against brute-force attacks.

Finally, encrypted findings indicated that the suggested method effectively prevented data leaking and ensured security.

Since the suggested method did not address key management or the storage and protection of the encryption keys, it also did not mention which component is responsible for generating and distributing the keys [53], [54]. Likewise, it skipped over the topic of how the roles are assigned to peers in the system.

Zuo et al. 2021 [55] employed an IoT architecture with blockchain technology for the monitoring and management of oil field equipment and operations. Furthermore, the system enabled machine-to-machine interactions for increased automation and control, fast data collection for remote conditional monitoring, and the execution of the best control actions to reduce facility downtime. Moreover, smart contracts were used to remotely monitor, operate, and assess the security features of the oil field.

Since blockchain storage is restricted, the suggested solution stores IoT data on a cloud server. As a result, the proposed method encountered storage constraints such as security concerns, as well as processing delays, particularly when retrieving data from the cloud server for the data integrity inspection process, resulting in a high response time.

Sobecki et al. 2022 [56] suggested a blockchain-based system for monitoring industrial infrastructure, especially chains/logistics and IoT/manufacturing. The concept intended to provide privacy-preserving, scalable, and effective data management for a wide range of applications, including healthcare and smart cities. The proposed scheme included: IoT devices generating logs and sending them to nodes, servers that accept sensor signals, collaborate to establish blockchain networks, and stored logs in an immutable format, systems or users can query nodes for individual data or aggregated results.

The study acknowledges the usage of consensus algorithms like Stellar Consensus Protocol (SCP) and Practical Byzantine Fault Tolerance (PBFT); however, it does not go into detail on the trade-offs between these algorithms and their applicability for particular use cases. The article did not do a full comparison of SCP and PBFT in terms of performance or efficiency.

The study of Zurkanain et al. 2023 [57] suggested a cloud-based platform, early warning system, and IoT-based pipeline monitoring system to monitor from a distance pipeline conditions for pipeline area. Through doing away with the need for wire in pipeline systems, this technology could save maintenance costs and requirements less by IoT platform support. A fully working prototype had been constructed with an emphasis on gas leak detection and monitoring systems. In this study, a variety of sensors were employed since the system needed to be detected and wirelessly configured. Every component answered underwent a functional test. This research elaborated on the security level system by offering an early warning system and the ability to monitor pipeline status via computer and smartphone. As an income, the system used Wireless Sensor Networks (WSNs) to collect, analyze, and transmit data wirelessly, removing the necessity for expensive cable technology, this allowed for effective monitoring of pipeline safety, integrity, dependability, and security.

Since the paper did not work in phases method, it omitted to produce key management or give a clarification in detail of the steps for registration and login process of the system components, or the data exchange way among them.

The suggested method of Kongsen et al. 2024 [58] buffered and transmitted patient vital signals using a global blockchain network due to the securely distributed database. An algorithm for the safe collection and sending of vital signs to the Ethereum network was included in the framework. Also, it introduced the subscribe or publish structure, which improved security while connecting to the blockchain network over the TLS channel. The distributed database's maintenance costs were analyzed, and the results highlighted how economical the method was. To sum up, the framework offered a very cost-effective and safe way to monitor healthcare remotely in situations of solitude at home.

The study failed to discuss the challenge of ensuring interoperability, among devices and healthcare systems. It overlooked the importance of integrating this system with healthcare systems and equipment. Furthermore, the article did not consider computing or communication costs, which may result in a lack of performance analysis.

Rodrigo B et al. 2024 [59] developed a decentralized blockchain-based architecture for monitoring resources in distributed systems, protecting privacy and data from cyberattacks in advanced contexts. Likewise, it used a smart contract-based monitoring system for real-time notifications, continuing surveillance, and responding to infrastructure observability demands. As well, a real-world research case was given to demonstrate the viability of leveraging blockchain technology with a Solo consensus algorithm which was a single node, to monitor in real-time for computing resources.

Despite the feature of the Solo consensus protocol algorithm that utilized by the proposed scheme. It suffered from centralization challenges due to being a single node as mentioned above. The decentralized structure of blockchain networks may be compromised by this centralization, leaving the network more open to manipulation and attacks.

5. Detection mechanisms

In 2021, the method of Kumar et al. 2021 [60] provided a scheme contained a blockchain and off-chain storage (IPFS) platform for storing multimedia items, such as images and videos as transactions. Also, the suggested system guaranteed multimedia assets' transparency, immutability, availability, and copyright protection using the perceptual hash algorithm. Besides, any peer was allowed to view its ledger and confirm the copyright data due to its complete distribution and having a consensus algorithm that the longest chain availability among the peers was used to distribute copyright information across the peers of the blockchain network.

By utilizing the perceptual hash (pHash) cryptography that makes small changes in images and videos were to be detected according to the proposed system. Despite that, the pHash might be cannot determine the modification in the presentation of the information. For instance, Rotation, cropping, and other changes that don't significantly affect the pHash value, could not be recognized by the system. Furthermore, false positives -- when the system incorrectly labels a legitimate video or image as tampered with.

The method of Peruman et al. 2023 [61] sought to identify and distinguish objects in border zones before securely transmitting that information to a cloud database using blockchain. As well, the method utilized blockchain with IoT devices to construct a tamper-proof and decentralized system for object detection. In this solution, IoT devices collected data from cameras, which were safely preserved in a cloud database protected by a blockchain ledger. The adoption of blockchain technology ensured that data was unalterable transparent, and only accessed by authorized individuals. That solution took advantage of the decentralized nature of blockchain technology to enable the safe sharing and storage of data acquired by cameras employed in an object detection system. The suggested method comprised the use of ESP 32 Cam for detecting drone or aircraft movements near border regions, automated vehicle detection, and feature extraction using CNNs.

The most important aspect was that the system may not fully address the issue of system scalability and massive data since it did not employ external storage to store video data. Furthermore, it may have significant retrieval delays during the integrity inspection process as a result of storing data in a cloud database.

Table 1. Illustrates comparison between researches

Security Features	Michael Kerr et al. 2018 [32]	Rong Wang et al. 2019 [5]	Khan et al. 2020 [34]	Tahir et al. 2021 [35]	Yan et al. 2021 [40]	Vivekanandan et al. 2021 [41]	Sobek et al. 2022 [56]	Zurkana et al. 2023 [57]	Yu et al. 2023 [42]	Zhang et al. 2024 [37]	Rodrigo B et al. 2024 [59]
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Unlinkability	No	No	No	No	Yes	Yes	No	No	Yes	No	No
Man In-The Middle attack (MITM)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Impersonate attack	No	No	No	No	Yes	Yes	No	No	Yes	No	No
Sniffing attack	No	No	No	Yes	Yes	No	Yes	No	No	No	No
dictionary attack	No	No	No	No	Yes	Yes	No	No	Yes	No	No
Eavesdropping attack	No	No	No	Yes	Yes	No	Yes	No	No	No	No
Insider attack	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Sybil attack	No	No	No	No	No	Yes	No	No	No	No	No
Eclipse attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Denial of service (DDOS) attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
51% attack	No	No	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes
External data storage	No	Yes	No	Yes	No	No	No	No	No	Yes	No
Data encryption at transmitting before storing process	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Computation / Communication costs	No	No	No	Yes	Yes	Yes	No	No	Yes	No	No

Table 2. Illustrates researchers' methods and tools

Researcher	Method	Blockchain type	Tools
Choi et al. 2020 [51]	A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology.	Private blockchain	Java script, SHA-256, Labview, Ethernet TCP/IP
Kumar et al. 2021 [60]	A secured distributed detection system based on IPFS and blockchain for industrial image and video data security.	Un mentioned	IPFS, SHA-1, MD5, perceptual hash, difference hash, wavelet hash

Sobecki et al. 2022 [56]	Privacy-Preserving, Scalable Blockchain-Based Solution for Monitoring Industrial Infrastructure in the Near Real-Time.	Steller / Hyperledger Fabric	Elliptic Curve Diffie Helman (ECDH), AES, CTR
Peruman et al. 2023 [61]	Blockchain-Based Deep Learning Object Detection System for Enhanced Security and Reliability.	Ethereum	Convolution Neural Network (CNN), SHA-256, Solidity, Python, Truffle, Metamask, Ganache
Kongsen et al. 2024 [58]	A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation.	Ethereum	Solidity, Python, Raspberry Pi, MQTT protocol
Ghani et al. 2024 [47]	Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning.	Ethereum	Solidity, Web3, Ganache

Table 3. Illustrates the analysis of the related work sections

Section	Author	Year	Methodology	Disadvantages
Surveillance Systems	Lee et al. [36]	2021	Utilized a secure Merkle tree using a blockchain-based multimedia intelligent video surveillance system that protects privacy, and addresses security and privacy issues in cloud-based intelligent surveillance systems.	A lack of security and performance analysis
	Zhang et al. [37]	2024	Used a blockchain-based aberrant data storage model for cereal and oil video monitoring, InterPlanetary File System (IPFS) to ensure data security that relieves the storage burden on the blockchain and investigated the YOLOv7-based target recognition technique.	Face a challenge in the storing process of this scheme, where it relied on saving all original video data on IPFS without encrypting them which led to potential attacks such as MITM, Replay, and Sniffing.
Authentication Mechanisms	Hwaitat et al. [43]	2023	A novel strategy for a large-scale Internet of Things system built on a permissions-based blockchain that offered users a lightweight authentication system and optimized data storage, used homomorphic encryption for to encrypt IoT data at the	Face a delay in data retrieval due to uploading the IoT-encrypted data to the cloud

	Chen et al. [77]	2024	<p>user's end and upload this data to the cloud. the research contributed by developing a unique Internet of Things strategy built on a trust-aware security method that connects exceptional IoT services while enhancing security and privacy.</p> <p>Blockchain-based method for IoT that prioritizes anonymous authentication and safe data transfer. It can withstand security concerns such as impersonation, man-in-the-middle, and denial-of-service attacks while lowering computational and communication costs.</p>	Face issues in terms of unnecessary and repeated data, resulting in a system overload due to transmitting large volumes of data on a regular basis.
Artificial Intelligence Systems	Mahalingam et al. [49]	2024	The system used Recurrent Neural Networks (RNN), Elliptic Cryptosystems (ECC), and blockchain technology to improve security, data privacy, and transparency in IoT-based intelligent agriculture systems, predict crop yields, identify pests and diseases, monitor weather trends, and enable secure communication between IoT devices.	Not obvious who is responsible for creating and distributing encryption/decryption keys over the network
	Hennebelle et al. [48]	2024	Offered end-to-end automated IoT-edge-AI-blockchain system for diabetes prediction using risk variables.	Did not present the registration process of patients and medical experts in detail.
Security mechanisms / Monitoring in different smart industries	Kongsen et al. [58]	2024	Collection and sending of vital signs to the Ethereum network, connecting to the blockchain network over the TLS channel, offered a very cost-effective and safe way to monitor healthcare remotely. Blockchain-based architecture for monitoring resources in distributed systems, used a smart contract-based	The challenge of ensuring interoperability
	Rodrigo B et al. [59]	2024	monitoring system for real-time notifications, utilized the Solo consensus algorithm which was a single node, to monitor in real-time for computing resources.	Centralization challenges due to being a single node in the Solo consensus algorithm.

Detection Mechanisms	Kumar et al. [60]	2021	Utilize a blockchain and off-chain storage (IPFS) platform for storing multimedia items. Use the perceptual hash algorithm for copyright protection of images, videos. Utilize a blockchain with IoT devices to construct a tamper-proof and decentralized system for object detection, IoT devices collected data from cameras, which were safely preserved in a cloud database protected by a blockchain ledger, use of ESP 32 Cam for detecting drone or aircraft movements near border regions, automated vehicle detection, and feature extraction using CNNs.	False positives -- when the system incorrectly labels a legitimate video or image as tampered with.
	Peruman et al. [61]	2023		The issues of system scalability and massive data since it did not employ external storage to store video data.

4. Conclusion:

Monitoring and surveillance systems are critical for the performance of various sectors. Their major purpose is to increase safety and improve inhabitants' quality of life. To provide a secure environment, a variety of tasks are required. However, from an IoT standpoint, cameras, sensors, and other monitoring devices may be utilized to achieve a variety of goals, including improving public security, successfully managing industries, and avoiding anomalous behavior. By strategically implementing these devices, such sectors may quickly monitor and respond to events, resulting in a safer and more comfortable urban environment for citizens. we introduced a review research that integrates monitoring and surveillance systems based IoT with blockchain technology. Besides, the research discussed the challenges that previous systems faced. Furthermore, our paper presented a comparison between the systems according to their method, tools that are utilized such as encryption algorithms, programming languages, and the types of blockchain. Moreover, Our research soke to make a comparison that includes security features such as mutual authentication, Anonymity, the employing of external storage, performance analysis that comprises the computation and communication costs, and attacks that the research papers neglected to address. Also, the research gave a summary and analysis of previous works. Lastly, the study benefits beginner researchers in terms of saving time and effort.

References

- [1] L. A. Ajao, J. Agajo, E. A. Adedokun, and L. Karngong, "Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry," J (Basel), vol. 2, no. 3, pp. 300–325, Aug. 2019, Doi: 10.3390/j2030021.
- [2] J. Aslam, A. Saleem, N. T. Khan, and Y. B. Kim, "Blockchain technology for oil and gas: implications and adoption framework using agile and lean supply chains," Processes, vol. 10, no. 12, p. 2687, 2022, Doi: <https://doi.org/10.3390/pr10122687>.
- [3] I. V Ngonadi and S. Ajiroghene, "Remote Pipeline Monitoring Security System," International Journal of Scientific Research in Computer Science, Engineering and

- Information Technology, vol. 7, no. 6, pp. 135–145, Dec. 2021, Doi: <https://doi.org/10.32628/CSEIT217631>
- [4] Y. Feng, “Dynamic Monitoring System of Oil Pipeline Leakage for Oil and Gas Safety,” in *Journal of Physics: Conference Series*, IOP Publishing, 2023, p. 012002, Doi:10.1088/1742-6596/2503/1/012002.
- [5] B. Gipp, J. Kosti, and C. Breiting, “Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain,” in *Mediterranean Conference on Information Systems (MCIS)*, 2016, pp. 1–11.
- [6] Rong Wang; Wei-Tek Tsai; Juan He; Can Liu; Qi Li; Enyan Deng and Institute of Electrical and Electronics Engineers, “A Video Surveillance System Based on Permissioned Blockchains and Edge Computing,” in *2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Rong Wang; Wei-Tek Tsai; Juan He; Can Liu; Qi Li; Enyan Deng, Ed., Japan: IEEE, May 2019, pp. 1–6. Doi: 10.1109/BIGCOMP.2019.8679354
- [7] D. R. Patrikar and M. R. Parate, “Anomaly detection using edge computing in video surveillance system: review,” *Int J Multimed Inf Retr*, vol. 11, no. 2, pp. 85–110, Jun. 2022, Doi: 10.1007/s13735-022-00227-8.
- [8] M. Chiang and T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” *IEEE Internet of Things Journal*, vol. 3, no. 6. Institute of Electrical and Electronics Engineers Inc., pp. 854–864, Dec. 01, 2016. Doi: 10.1109/JIOT.2016.2584538.
- [9] J. Dai, Q. Li, H. Wang, and L. Liu, “Understanding images of surveillance devices in the wild,” *Knowl Based Syst*, vol. 284, p. 111226, 2024, Doi:<https://doi.org/10.1016/j.knosys.2023.111226>.
- [10] W. El-Shafai, M. A. Fouda, E. S. M. El-Rabaie, and N. A. El-Salam, “A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends,” *Multimed Tools Appl*, vol. 83, no. 2, pp. 4241–4307, Jan. 2024, Doi: 10.1007/s11042-023-15609-1.
- [11] R. A. Michelin, N. Ahmed, S. S. Kanhere, A. Seneviratne, and S. Jha, “Leveraging lightweight blockchain to establish data integrity for surveillance cameras,” in *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)*, IEEE, 2020, pp. 1–3. Doi: 10.1109/ICBC48266.2020.9169429.
- [12] S. M. Umran, S. Lu, Z. A. Abduljabbar, Z. Lu, B. Feng, and L. Zheng, “Secure and Privacy-preserving Data-sharing Framework based on Blockchain Technology for Al-Najaf/Iraq Oil Refinery,” in *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, IEEE, 2022, pp. 2284–2292. Doi:10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00325.
- [13] S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, “Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry,” *Internet of Things*, vol. 24, p. 100969, 2023, Doi:<https://doi.org/10.1016/j.iot.2023.100969>.

- [14] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, "Secure data of industrial internet of things in a cement factory based on a Blockchain technology," *Applied Sciences*, vol. 11, no. 14, p. 6376, 2021, Doi: <https://doi.org/10.3390/app11146376>.
- [15] S. M. Umran, S. Lu, Z. A. Abduljabbar, and X. Tang, "A Blockchain-Based Architecture for Securing Industrial IoTs Data in Electric Smart Grid," *Computers, Materials and Continua*, vol. 74, no. 3, pp. 5389–5416, 2023, Doi: [10.32604/cmc.2023.034331](https://doi.org/10.32604/cmc.2023.034331).
- [16] M. Sabeeh and A. adil Yassin, "Secure Electronic Healthcare Record based on Distributed Global Database and Schnorr Signcryption," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 19, pp. 62–69, Jan. 2023, Doi: [10.37917/ijeee.19.1.8](https://doi.org/10.37917/ijeee.19.1.8).
- [17] A. Alfghan, T. Moulahi, and A. Alabdulatif, "Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT)," *Blockchain: Research and Applications*, vol. 2, no. 4, p. 100036, 2021, Doi: <https://doi.org/10.1016/j.bcra.2021.100036>.
- [18] A. Kuznetsov, I. Oleshko, V. Tymchenko, K. Lisitsky, M. Rodinko, and A. Kolhatin, "Performance analysis of cryptographic hash functions suitable for use in blockchain," *International Journal of Computer Network & Information Security*, vol. 13, no. 2, pp. 1–15, 2021. Doi: [10.5815/ijcnis.2021.02.01](https://doi.org/10.5815/ijcnis.2021.02.01).
- [19] Y. Genç and E. Afacan, "Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA)," in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, IEEE, 2021, pp. 1–6. Doi: [10.1109/IEMTRONICS52119.2021.9422589](https://doi.org/10.1109/IEMTRONICS52119.2021.9422589).
- [20] W. Ren, X. Wan, and P. Gan, "A double-blockchain solution for agricultural sampled data security in Internet of Things network," *Future Generation Computer Systems*, vol. 117, pp. 453–461, 2021, Doi: <https://doi.org/10.1016/j.future.2020.12.007>.
- [21] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative IPFS-based storage model for blockchain," in *2018 IEEE/WIC/ACM international conference on web intelligence (WI)*, IEEE, 2018, pp. 704–708. Doi: [10.1109/WI.2018.000-8](https://doi.org/10.1109/WI.2018.000-8).
- [22] C. J. F. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols," in *Computer Aided Verification*, A. Gupta and S. Malik, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 414–418. Doi: https://doi.org/10.1007/978-3-540-70545-1_38.
- [23] N. 'Dalal, J. 'Shah, K. 'Hisaria, and D. 'Jinwala, "A Comparative Analysis of Tools for Verification of Security Protocols," *Int. J. Communications, Network and System Sciences*, pp. 779–787, Oct. 2010, doi: [10.4236/ijcns.2010.310104](https://doi.org/10.4236/ijcns.2010.310104).
- [24] D. Bhanushali, A. Koul, S. Sharma, and B. Shaikh, "BlockChain to Prevent Fraudulent Activities: Buying and Selling Property Using BlockChain," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 705–709. doi: [10.1109/ICICT48043.2020.9112478](https://doi.org/10.1109/ICICT48043.2020.9112478).
- [25] R. Verma, N. Dhanda, and V. Nagar, "Application of Truffle Suite in a Blockchain Environment," in *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*, P. K. Singh, S. T. Wierchoń, S. Tanwar, J. J. P.

- C. Rodrigues, and M. Ganzha, Eds., Singapore: Springer Nature Singapore, 2023, pp. 693–702, Doi: https://doi.org/10.1007/978-981-19-1142-2_54.
- [26] Z. Wang, X. Chen, X. Zhou, Y. Huang, Z. Zheng, and J. Wu, “An empirical study of solidity language features,” in 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), IEEE, 2021, pp. 698–707. Doi: 10.1109/QRS-C55045.2021.00105.
- [27] A. J. Dhruv, R. Patel, and N. Doshi, “Python: the most advanced programming language for computer science applications,” Science and Technology Publications, Lda, pp. 292–299, 2021. Doi: 10.5220/0010307900003051.
- [28] A. Fitwi and Y. Chen, “Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain,” in 2021 International Conference on Computer Communications and Networks (ICCCN), Apr. 2021, pp. 1–8. [Online]. Available: <http://arxiv.org/abs/2104.05617>, Doi: 10.1109/ICCCN52240.2021.9522199.
- [29] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, “A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology,” in 2018 IEEE International Smart Cities Conference (ISC2), Jul. 2018, pp. 1–4. [Online]. Available: <http://arxiv.org/abs/1807.07487>, Doi: 10.1109/ISC2.2018.8656968.
- [30] Michael Kerr, Fengling Han, and Ron van Schyndel, “A Blockchain Implementation for the Cataloguing of CCTV Video Evidence,” in 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018, pp. 1–6. Doi: 10.1109/AVSS.2018.8639440.
- [31] R. Uda, “Data Protection Method with Blockchain against Fabrication of Video by Surveillance Cameras,” in Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, 2020, pp. 29–33, Doi: <https://doi.org/10.1145/3390566.3391685>.
- [32] P. W. Khan, Y.-C. Byun, and N. Park, “A data verification system for CCTV surveillance cameras using blockchain technology in smart cities,” Electronics (Basel), vol. 9, no. 3, p. 484, 2020 Doi: <https://doi.org/10.3390/electronics9030484>.
- [33] M. Tahir, M. N. Asghar, N. Kanwal, B. Lee, and Y. Qiao, “Joint Crypto-Blockchain Scheme for Trust-Enabled CCTV Videos Sharing,” in Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 341–345. Doi: 10.1109/Blockchain53845.2021.00054.
- [34] D. Lee and N. Park, “Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree,” Multimed Tools Appl, vol. 80, no. 26–27, pp. 34517–34534, Nov. 2021, Doi: 10.1007/s11042-020-08776-y.
- [35] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K. K. R. Choo, “HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes,” IEEE Internet Things J, vol. 7, no. 2, pp. 818–829, Feb. 2020, Doi: 10.1109/JIOT.2019.2944400.
- [36] X. Yang et al., “Blockchain-based secure and lightweight authentication for Internet of Things,” IEEE Internet Things J, vol. 9, no. 5, pp. 3321–3332, 2021. Doi: 10.1109/JIOT.2021.3098007.

- [37] M. Vivekanandan, S. VN, and S. R. U, "BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology," *Peer Peer Netw Appl*, vol. 14, pp. 403–419, 2021, Doi:<https://doi.org/10.1007/s12083-020-00963-w>.
- [38] L. Yu, M. He, H. Liang, L. Xiong, and Y. Liu, "A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services," *Sensors*, vol. 23, no. 3, p. 1264, 2023, Doi:<https://doi.org/10.3390/s23031264>.
- [39] R. Vamshidhar Reddy, V. Jaya prakash Reddy, and E . Madhusudhana Reddy, "Automatic Face Expressions and Gesture Detection System Using Blockchain Security," in *2020 International Conference on Intelligent Engineering and Management (ICIEM-2020)*, 2020, pp. 1–5, Doi: 10.1109/ICIEM48762.2020.9160325.
- [40] P. Jain et al., "Blockchain-Enabled Smart Surveillance System with Artificial Intelligence," *Wirel Commun Mob Comput*, vol. 2022, 2022, Doi:<https://doi.org/10.1155/2022/2792639>.
- [41] A. Hennebelle, L. Ismail, H. Materwala, J. Al Kaabi, P. Ranjan, and R. Janardhanan, "Secure and privacy-preserving automated machine learning operations into end-to-end integrated IoT-edge-artificial intelligence-blockchain monitoring system for diabetes mellitus prediction," *Comput Struct Biotechnol J*, vol. 23, pp. 212–233, Dec. 2024, Doi: 10.1016/j.csbj.2023.11.038.
- [42] N. Mahalingam and P. Sharma, "An intelligent blockchain technology for securing an IoT-based agriculture monitoring system," *Multimed Tools Appl*, vol. 83, no. 4, pp. 10297–10320, Jan. 2024, Doi: 10.1007/s11042-023-15985-8.
- [43] K. A.-A. Mutlaq, V. O. Nyangaresi, M. A. Omar, and Z. A. Abduljabbar, "Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment," in *Applied Cryptography in Computer and Communications*, J. Lin and Q. Tang, Eds., Cham: Springer Nature Switzerland, 2022, pp. 46–64, Doi:https://doi.org/10.1007/978-3-031-17081-2_4.
- [44] M. K. Choi, C. Y. Yeun, and P. H. Seong, "A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology," *IEEE Access*, vol. 8, pp. 118732–118740, 2020, Doi: 10.1109/ACCESS.2020.3005134.
- [45] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, Feb. 2020, Doi: 10.3390/e22020175.
- [46] V. O. Nyangaresi et al., "Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges," in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2021, pp. 1–6. Doi: 10.1109/ICECET52533.2021.9698744.
- [47] V. O. Nyangaresi, Z. A. Abduljabbar, S. H. A. Refish, M. A. Al Sibahee, E. W. Abood, and S. Lu, "Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids," in *Cognitive Radio Oriented Wireless Networks and Wireless Internet*, H. Jin, C. Liu, A.-S. K. Pathan, Z. Md. Fadlullah, and S. Choudhury, Eds., Cham: Springer International Publishing, 2022, pp. 325–340, Doi:https://doi.org/10.1007/978-3-030-98002-3_24.

- [48] Y. Zuo and Z. Qi, “A Blockchain-based IoT Framework for Oil Field Remote Monitoring and Control,” IEEE access, vol. 10, pp. 2497–2514, 2021. Doi: 10.1109/ACCESS.2021.3139582.
- [49] A. Sobecki, S. Barański, and J. Szymański, “Privacy-Preserving, Scalable Blockchain-Based Solution for Monitoring Industrial Infrastructure in the Near Real-Time,” Applied Sciences (Switzerland), vol. 12, no. 14, Jul. 2022, Doi: 10.3390/app12147143.
- [50] M. A. Zurkanain and S. K. Subramaniam, “Investigation and Implementation of IoT Based Oil & Gas Pipeline Monitoring System,” International Journal of Recent Technology and Applied Science (IJORTAS), vol. 5, no. 1, pp. 1–11, Mar. 2023, Doi: 10.36079/lamintang.ijortas-0501.477.
- [51] J. Kongsen, D. Chantaradsuwan, P. Koad, M. Thu, and C. Jandaeng, “A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation,” Journal of Sensor and Actuator Networks, vol. 13, no. 1, p. 13, Feb. 2024, Doi: 10.3390/jsan13010013.
- [52] Rodrigo B, “Towards a Decentralized Blockchain-Based Resource Monitoring Solution For Distributed Environments,” Journal of Internet Services and Applications, vol. 15, p. 1, 2024, Doi: 10.5753/jisa.2024.3813.
- [53] P. M. Peruman, G. Krishnan, M. Gopinath, and S. Dharanidar, “Blockchain-Based Deep Learning Object Detection System for Enhanced Security and Reliability,” in 2023 International Conference on System, Computation, Automation and Networking, ICSCAN 2023, Institute of Electrical and Electronics Engineers Inc., 2023. Doi: 10.1109/ICSCAN58655.2023.10395763.
- [54] Y. Zhang et al., “Research on Blockchain-Based Cereal and Oil Video Surveillance Abnormal Data Storage,” Agriculture (Switzerland), vol. 14, no. 1, Jan. 2024, Doi: 10.3390/agriculture14010023.
- [55] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, “A secured distributed detection system based on IPFS and blockchain for industrial image and video data security,” J Parallel Distrib Comput, vol. 152, pp. 128–143, Jun. 2021, Doi:10.1016/j.jpdc.2021.02.022.
- [56] M. A. N. U. Ghani et al., “Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning,” Mathematical Biosciences and Engineering, vol. 21, no. 3, pp. 4165–4186, 2024, Doi: 10.3934/mbe.2024184.

أنظمة المراقبة والمراقبة القائمة على إنترنت الأشياء مع Blockchain: مراجعة الأدبيات

نور علي الشريفي¹، علي عادل ياسين^{1*}، زيد أمين عبد الجبار¹، فنسنت أومولو نيانجاري^{2,3}

¹ قسم علوم الحاسب ، كلية التربية للعلوم الصرفة ، جامعة البصرة ، البصرة 61004 ، العراق.

² قسم علوم الكمبيوتر وهندسة البرمجيات ، جامعة جاراموغي أوجينجا أودينغا للعلوم والتكنولوجيا ، بوندو 40601 ، كينيا.

³ قسم الإلكترونيات التطبيقية ، كلية سافيتا للهندسة ، SIMATS ، تشيناي ، تامي لنادو 602105 ، الهند.

المخلص

معلومات البحث

على الصعيد العالمي ، تطورت التكنولوجيا في مختلف القطاعات لتحسين نوعية حياة الأفراد وسلامتهم. تعد أنظمة المراقبة والمراقبة من المكونات الهامة في البنية التحتية للصناعات المختلفة. تحسنت أنظمة المراقبة والمراقبة القائمة على إنترنت الأشياء على الفور في السنوات الأخيرة ، حيث تتكامل مع التقنيات المتطورة مثل blockchain والتعلم العميق والحوسبة السحابية والحوسبة المتطورة. على حد علمنا ، هناك عدد قليل من المراجعات في مجال blockchain القائم على المراقبة والمراقبة. لهذا السبب ، أجرينا مراجعة الأدبيات لمناقشة الطرق المختلفة لمعالجة مشاكل الأمان والخصوصية في أنظمة المراقبة والمراقبة القائمة على إنترنت الأشياء باستخدام تقنية blockchain. يقسم بحثنا الأوراق إلى خمسة أقسام وهي أنظمة المراقبة وآليات المصادقة والذكاء الاصطناعي وآليات الأمان / المراقبة في الصناعات الذكية المختلفة وآليات الكشف. كما يركز على استخدام تقنية البلوك تشين وأنواعها، وتوظيف تخزين البيانات الخارجية التي تتكامل مع البلوك تشين لدعم تخزينها، ونوع الأدوات المستخدمة، لمقارنة الدراسات السابقة. بالإضافة إلى ذلك ، يقارن الاستعراض المنهجي الحالية من حيث أوجه القصور مثل نقص التحليل الأمني وتقييم الأداء والهجمات الضارة وأمن البيانات أثناء الإرسال. يقدم بحثنا مقارنة تتضمن ميزات الأمان مثل المصادقة المتبادلة ، وإخفاء الهوية ، واستخدام التخزين الخارجي ، وتحليل الأداء ، كما قدم البحث ملخصاً وتحليلاً للأعمال السابقة. أخيراً ، تفيد الدراسة الباحثين المبتدئين من حيث توفير الوقت والجهد.

الاستلام 22 نيسان 2024

المراجعة 8 تموز 2024

القبول 25 تموز 2024

النشر 31 كانون الاول 2024

الكلمات المفتاحية

أنظمة المراقبة ، المراقبة في الوقت الفعلي ، Blockchain ، إنترنت الأشياء.

Citation: N. A. Alshuraify et al., J. Basrah Res. (Sci.) 50(2), 42 (2024).

DOI:<https://doi.org/10.56714/bjrs.50.2.5>

*Corresponding author email : pgs.ali.yassin@uobasrah.edu.iq

