electronics

MDPI

Article

A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities

Prince Waqas Khan [1], Yung-Cheol Byun [1,*] and Namje Park[2]

[1] Department of Computer Engineering, Jeju National University, Jeju-si 63243, Korea; princewaqas12@hotmail.com

[2] Department of Computer Education, Teachers College, Jeju National University, Jeju City 63243, Korea; namjepark@jejunu.ac.kr

* Correspondence: ycb@jejunu.ac.kr

Received: 27 February 2020; Accepted: 11 March 2020; Published: 15 March 2020

Abstract: The video created by a surveillance cameras plays a crucial role in crime prevention and examinations in smart cities. The closed-circuit television camera (CCTV) is essential for a range of public uses in a smart city; combined with Internet of Things (IoT) technologies they can turn into smart sensors that help to ensure safety and security. However, the authenticity of the camera itself raises issues of building up integrity and suitability of data. In this paper, we present a blockchain-based system to guarantee the trustworthiness of the stored recordings, allowing authorities to validate whether or not a video has been altered. It helps to discriminate fake videos from original ones and to make sure that surveillance cameras are authentic. Since the distributed ledger of the blockchain records the metadata of the CCTV video as well, it is obstructing the chance of forgery of the data. This immutable ledger diminishes the risk of copyright encroachment for law enforcement agencies and clients users by securing possession and identity.

Keywords: blockchain; smart city; CCTV; Hyperledger Fabric; video surveillance system; Internet of Things

1. Introduction

The prompt emergence of surveillance systems within metropolitan areas and services has been required to fulfill the necessities of the people for a better quality of life. Appropriately, there has been a remarkable evolution of digital devices, for example, smartphones, sensors, smart applications, actuators, and intelligent machines, which led to clear business goals for the Internet of Things (IoT) industry. Now it is conceivable to interconnect all nodes and build connections between them over the internet. The smart city is getting more intelligent than in the past due to the modern development of computer-aided technologies. Smart cities incorporate diverse kinds of electronic applications; for example, cameras in an observing framework, and sensors in a transportation framework. A smart city framework upgraded by the IoT innovation turns into a revolutionary idea; it likewise gets new concerns about the security of the information. Closed-circuit television cameras (CCTV) have emerged as the essential component of a smart city [1].

A CCTV system within a smart city may involve hundreds or thousands of IP based IoT cameras that operate 7 × 24 and generate a vast amount of digital content daily. The number of public and private CCTV is increasing day by day. Additionally, with improving image processing technology, it is possible to obtain diverse information [2]. Recently, CCTV has been helping in many sectors of life. Therefore, it is necessary to ensure CCTV image integrity. The present control method and the dynamic multimedia innovation advancement made it conceivable in any event, for a fledgling to effectively erase an item from a video sequence. It is also possible to include an article from another video source or to add an article created by illustrations in programming software. The improvement of image analysis innovation via artificial intelligence CCTV, is likewise effectively underway. With the ascent of artificial intelligence (AI) and profound learning methods, the presence of advanced counterfeiting has multiplied in recent years. Now, deepfakes have the capability of modifying reality and disintegrating trust by giving false reality [3]. A built-in video compression algorithm is usually used in surveillance cameras. To forge a video, the intruder has to decompress the video, change its data, and re-compress again. It can be analyzed by the noise characteristics of frame compression [4].

Blockchain is overwhelming the world, to a great extent, because of the achievement of digital currency. A blockchain, also called a distributed ledger, is a write-only data structure kept up by a lot of nodes that do not wholly confide in one another. Many studies combine blockchain and image and video processing algorithms. Applications include combating deepfake videos [5], medical image processing [6], image encryption [7], and digital content rights management [8]. A decentralized solution based on blockchain for digital video obtained by dashboard cameras is presented by [9]. The presented technique enables proving that video has not been tampered based on time stamping, allowing it to be presented as proof in the court. Blockchain innovation's core segment is an innovative protocol that empowers information to be traded among different entities inside a system. As such, it does not require any intermediaries, since system members are connected with encrypted identities and legitimately with one another utilizing distributed communication. Each transaction is then added to a changeless ledger chain and distributed to every node. With the ascent of information breaches, extortion, and fraud, a number of projects are utilizing blockchain innovation for document and identity approval [10]. Validation through blockchain is achieved through end-to-end encryption, time-stamping, and checking for legitimacy. Table 1 shows the existing state of knowledge articles and proposed gap, which we intend to fill for smart cities.

Table 1. Blockchain based research articles for smart cities.

Sr # [Ref.]	Year	Blockchain Platform	Date Type	Description
1 [11]	2016	Ethereum	Medical history	Patients' personal immutable medical record
2 [12]	2017	Bitcoin	User data	User-centric access control of personal data
3 [13]	2017	Hyperledger Fabric	Anonymized dataset	Consensus based data transfer between data broker and data receiver
4 [14]	2017	Ethereum	Distributed energy resources	Distributed energy resources control system for smart grids
5 [15]	2017	Multichain	Electricity	proof-of-concept based blockchain for electricity trading in smart industry
6 [16]	2017	Block-VN	Vehicular information	Distributed network of vehicles in smart city
7 [17]	2017	BigchainDB	Supply chain data	Storage of products data of food supply chain
8 [18]	2017	Hyperledger Fabric	Video	Smart contract and network service based blockchain for video delivery
9 [19]	2018	Ethereum	E-voting	A Secure electronic voting system based on blockchain
10 [20]	2019	Hyperledger Fabric	Drug records	Integrity management of drug supplyChain for smart hospitals
Proposed	-	Hyperledger Fabric	Video , meta data	Data Verification System For CCTV Surveillance Camera for Smart cities

In this paper, we suggest a system model that can manage, use, and authenticate CCTV. This model allows a CCTV's data center to verify a CCTV film and surveillance camera. We structured and executed a procedure that can more reliably check video forgery and detect forgery by applying high-security blockchain technology to CCTV. Specifically, by dispersing and sharing a number of CCTV pictures among blockchain participating nodes, it is conceivable to limit the issue of a single point of failure, which is a blockchain advantage. It can also be recognized as evidence under criminal law. A single point of failure is one issue that can make the whole framework stop working. It can be brought about by a variety of factors, including machine malfunctions, purposeful or accidental human behavior, and power outages.

The remainder of this paper is organized as follows: Section 2 provides the existing research. Section 3 describes materials and methods, which include the introduction of blockchain technology and details about the proposed scheme. Section 4 describes the obtained simulation results and analyses. Section 5 presents a discussion about our proposed system. Finally, Section 6 concludes this paper.

2. Related Work

Smart Cities are seen as ecosystems that are commonly characterized as networks of associating devices and their surroundings, and are ordinarily depicted as perplexing systems shaped in light of resource interdependencies. Gretzel et al. [21] included four progressively essential components that exist in this ecosystem's definition of a smart city. These are interaction or engagement, balance, loosely coupled actors with shared objectives, and finally, self-organization. Numerous IoT gadgets need memory and computational complexities to cope with modern computing devices. Lack of computational power makes them defenseless against a broad scope of cyber attacks. Javaid et al. [22] displayed an IoT device and server correspondence framework using at Ethereum. They addressed the issue of security issues related to distributed denial of service (DDOS) attacks in the IoT system. They utilized a modified smart contract that empowers a superior resistance mechanism against DDoS and rogue device assaults. Kim et al. [23] presented an idea of using blockchain technology to solve the security issues of a sensor-based platform. IoT devices are the main components of smart homes, smart factories, and intelligent appliances, which are of great importance. They also concluded that the global market of sensors is expected to grow up to 220 trillion KRW by 2021. So it very important to solve the issue of a substantial sensor market. They proposed a blockchain-based authentication protocol to address security issues. By using that protocol, the IoT environment can become efficient and stable. Heng et al. [24] used the smart contract of Hyperledger Fabric for the task management of sensors. They used this feature of blockchains in the IoT environment to ensure the verification at runtime of sensors and actuators. The use of smart contracts makes it easy to automate the business logic and helps in time-saving with the surety of zero error.

Substantial work has been done in the field of video forensics. This advancement allows the video evidence to be used in court cases. Recent techniques used for video forgery detection are mainly based on an autoencoder with recurrent convolutional neural networks, an auto-encoder with a goturn algorithm, watermarking techniques, and digital signatures. Reference [25] proposed an autoencoders and recurrent neural networks based architecture to detect the video forgery. They trained a long short-term memory (LSTM) model to exploit dependencies. Reference [26] introduces a model to identify the trustworthiness of digital videos using an auto-encoder with a goturn algorithm. Zheng et al. [27] used the watermarking system of authenticating the sensor data. In their work, they combine spatial and temporal watermarking to obtain compression survival authentication. Sowmya et al. [28] discussed the spatio-temporal triad feature relationship to authenticate a video. They generated a unique content-based signature to detect inter and intraframe forged videos. In expansion, regardless of whether an image examination innovation is created, there are numerous instances of breakdown because of the restriction of the sensor. It can likewise happen when controlling images for harmful purposes. [29] explored the correlations between the noise residues at the neighboring blocks level. They also used the Bayesian classifier to get an optimal threshold value. However, this technique can miscalculate the forgery in case of a calculation error in noise residues. In [30], multiple feature hashing is introduced to deal with the accuracy issues of near-duplicate video retrieval (NDVR). They introduced content-based video hashing methods to ensure the authenticity of video features. However, their approach is sensitive towards the manipulation of content and more focused on video retrieval and identification instead of content-preserving manipulations.

In expansion, an assortment of reasons undermines the respectability of video information caught on CCTV [31]. On the other hand, CCTV-based administrations are being reinforced and diversified. Therefore, to offer assistance accurately, the trustworthiness of an image was observed by Kwon and his associates [32]. The Privacy Act takes into account the establishment of CCTVs for public places, which requires reaching out to the proprietors of CCTVs to get video information. However, this procedure takes a lot of time. Regardless of whether a video is procured, it is hard to use in open organizations because the video is not ensured to be an original video that it has not been manipulated. Panwar et al. [33] proposed a structure to give sensor information confirmation through cryptographic algorithms implementing a log sealing system and creating permanent pieces of evidence utilized for log verification. The structure guarantees that sensor information and log-fixed data could be put away in untrusted storage with the proposed verification system ensuring its integrity. However, this structure depends on the reliability in the instrument; for example, Intel SGX to store the fixed data in an incorporated way. False news has become a global issue that raises extreme difficulties for human culture and the majority rules system. This issue has emerged because of the development of various accompanying technological marvels. Qayyum et al. [34] have presented the cutting edge—to the point of producing disquietude—of realistic-looking fake data and concentrated explicitly on the marvels of fake news. To address the fake news issue, they have proposed a blockchain-based structure for the identification and alleviation of fake news. They have portrayed a significant level of plan for our answer. They recommend a significant level diagram of a blockchain-based system for counterfeit news avoidance and feature the different structural issues and considerations regarding such a blockchain-based structure for handling fake news.

A video record assumes a critical job in giving proof to crime scenes or street mishaps. In any case, the principle issue with the video record is that it is regularly vulnerable against different video altering attacks. Ghimire et al. [35] proposed an integrity verification strategy dependent on a blockchain. In their approach, video content with foreordained fragments is key-hashed in a constant way and put away in a sequentially fastened manner along these lines, building up a database. However, they did not discuss the spectrum of the proposed approach, and implementation details were also missing. Kerr et al. [36] exhibited a practical execution of blockchain technology implemented to the assignment of analyzing CCTV video proof. Their prototype method worked great in production circumstances and demonstrated promising review and dependability properties. However, the visible watermark can not be recommended as a secure solution to protect the video from forgery. The addition of new nodes and the participants' verification method was also not discussed. In our proposed approach, we have addressed the existing limitations.

3. Materials and Methods

We have used the blockchain platform for the authenticity and verification of data for smart cities. In this section, we explain the flow of the proposed platform and its components in detail. Figure 1 illustrates the flow of our proposed model. It starts with the enrollment of users and registration of the devices. The membership service provider (MSP) assigns a unique key to every peer of the system. Only valid devices and users can access the system. We are using a Hyperledger Fabric that is a private blockchain, and it is different from public blockchain, in terms of user access. In a public blockchain, any user can enroll in the system, but in private, only valid users who have the private key assigned by the system admin can access the system. The proposed system gets the video and metadata of the imaging sensor and encrypts that data. After encryption, it makes a block, and every block is endorsed by endorsing peers. In Hyperledger Fabric, there is no consensus algorithm or no mining of the blocks. But to meet the validation purpose, there are validation peers who are nominated by the system admin. The valid use can generate requests through REST API to access the digital data from the blockchain.

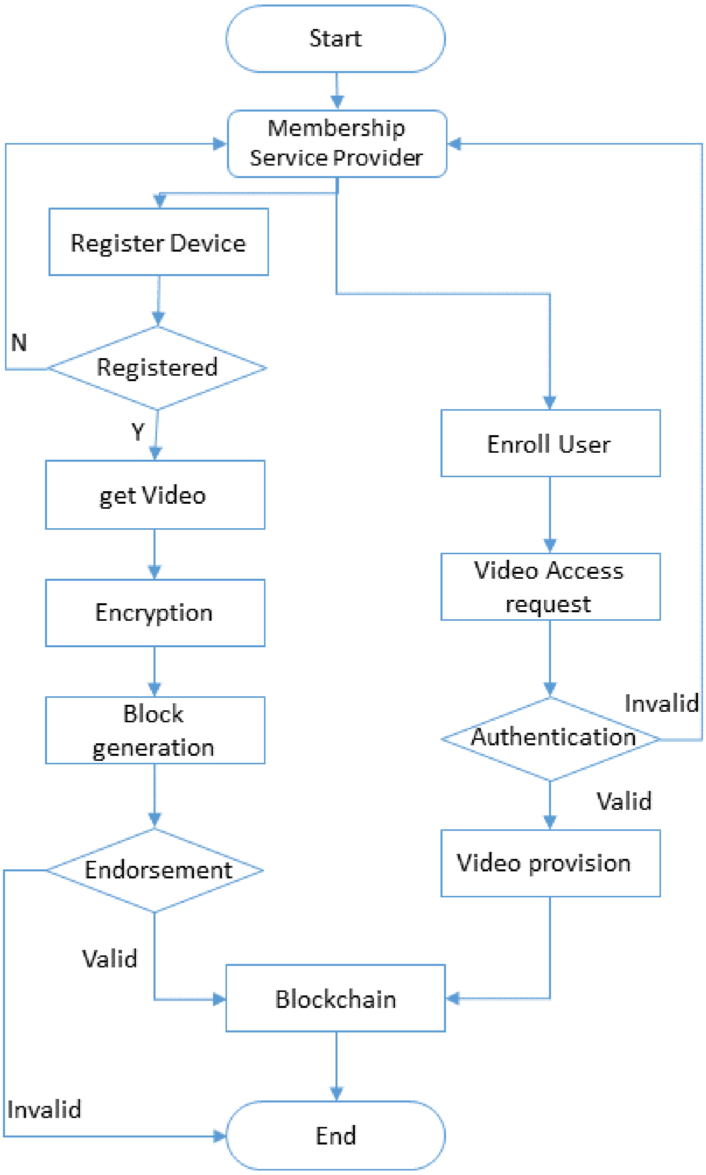


Figure 1. Flowchart of the proposed system.

3.1. *Blockchain Technology*

A blockchain emulates a central computing service through a distributed protocol, run by nodes connected over the Internet. The blockchain technically is replacing current centralized ledger systems with the decentralized ledgers. A blockchain uses encryption techniques, and it does not have the involvement of a third part, which makes it reliable [37]. A blockchain is composed of a chain of data block. Blocks can be composed and read by specific members, and entries are changeless, transparent, and accessible. Transactions are recorded in sequential order on a consistently developing database. A system of computers is associated through the web, wherein clients at any computer can get or send a data to another computer. Information is duplicated and put away over the framework over a shared system. It encourages shared exchange of significant worth without a central intermediary [38].

Hyperledger Fabric is an open source distributed ledger platform for private blockchains [39]. It offers a great scalability and it has been used in many fields of life.

Blockchain technology is relied upon to offer tremendous potential for bringing radical changes in a broad scope of enterprises, business models, and working procedures; for example, installment, bookkeeping, and inspecting. From the perspective of its specialized, multifaceted nature and the need for acknowledging these sweeping changes in the private, public, and commercial areas, this innovation, in the same way as other disruptive advancements previously, will get on gradually with a reasonable increment of pace over time [40]. The current focal point of blockchain innovation is essentially on utilizing it to approve, execute, and store transactions, which is the reason its improvement has been fundamentally driven by the money-related industries. Still, it is currently spreading across the further markets.

3.1.1. Important Features Of Blockchain Technology

Figure 2 shows the important basic features of a blockchain.

- **Replicated ledger:** In the blockchain, data is not stored on a central point. Blocks are distributed and replicated among the nodes. Each node contains a copy of the complete ledger. It eliminates the risks of data loss.
- **Cryptography:** Data, which is stored on the blockchain, is encrypted by its strong encryption algorithms. Hence, the integrity of all transactions and data is supported with digital signatures.
- **Consensus:** Every block contains a different number of transactions. Transactions need to be validated before adding to the existing blocks. In Hyperledger Fabric, there are validating nodes that validate every block before adding them into the chain.
- **Smart contract:** Blockchain provides an electronic version of the contract between two parties. The smart contract is computer code intended to digitally facilitate, verify, or enforce the negotiation.
- **Decentralization:** All transactions are shared without centralized control. Decentralization provides the trust and safety of the data.

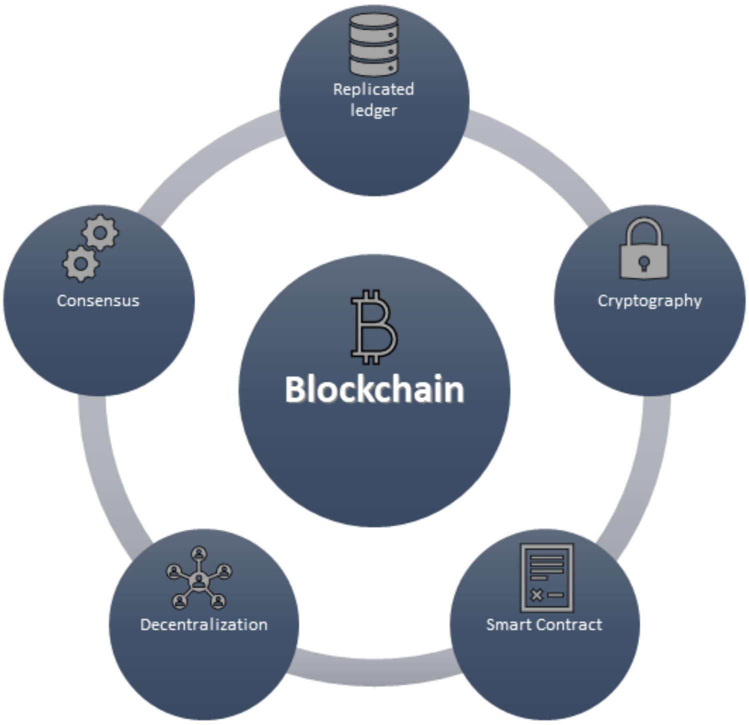


Figure 2. Important features of a blockchain.

3.1.2. Block

The genesis block is the very first block in a blockchain. It is the opening point for the ledger, though it does not hold any user transactions [41]. Instead, it includes an initial state of the network within the configuration transaction. Block comprises three sections: the header, transaction, and metadata. Metadata are written when a block is created. Figure 3 depicts a white box diagram of the K_{th} block of a blockchain.

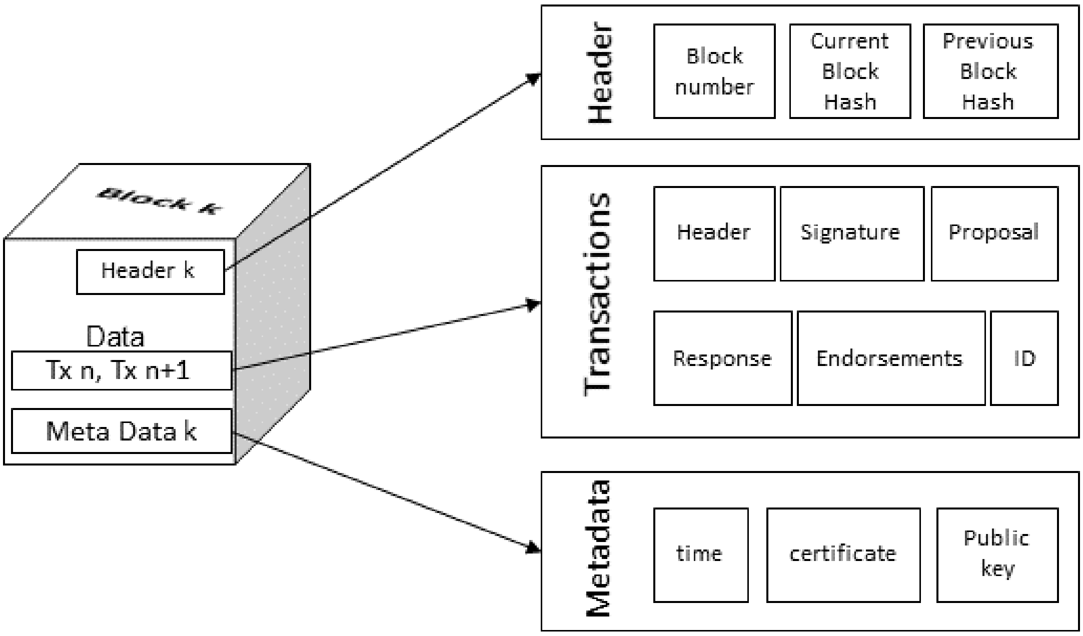


Figure 3. White box diagram of a block.

The header of the block captures some essential information about the transaction. It contains the current block number, the hash of the current block, and the hash of the previous block. The data within the blockchain include different transactions [42]. Each transaction consists of a unique ID, header, cryptographic signature, proposal, response, and endorsement. Input parameters provided by an application to the smart contract are encoded in the proposal, which forms the suggested ledger update. The response obtains the before and after cases of the world state, as a read write set (RW-set). It is the product of a smart contract, and if the transaction is successfully verified, it will be implemented on the ledger to renew the world state. The endorsement is a list of signed transaction acknowledgments from every required organization, adequate to meet the endorsement policy. Block metadata includes a certificate, a public key, the writing time of the block, and the signature of the block writer.

3.1.3. Transactions

Figure 4 shows the process of transaction processing by application in Hyperledger Fabric v1.4. Before initiating a transaction, the authentication of the application by the membership service provider (MSP) is completed [43]. The authenticated client app starts the transaction process by connecting to the peer. After connecting, it invokes the transaction proposal to said peer. The peer then invokes the chaincode with that proposal, and the chaincode generates the requested query for the ledger. The chaincode can also propose a ledger update. The ledger sends back the response to the peer, which further forwards this response to the application. After receiving the request, the response application generates a claim that a transaction should be ordered to the orderer. The orderer collects transactions from the network, generates blocks, and sends them to all peers. The peer receives the block and updates the ledger after verification.

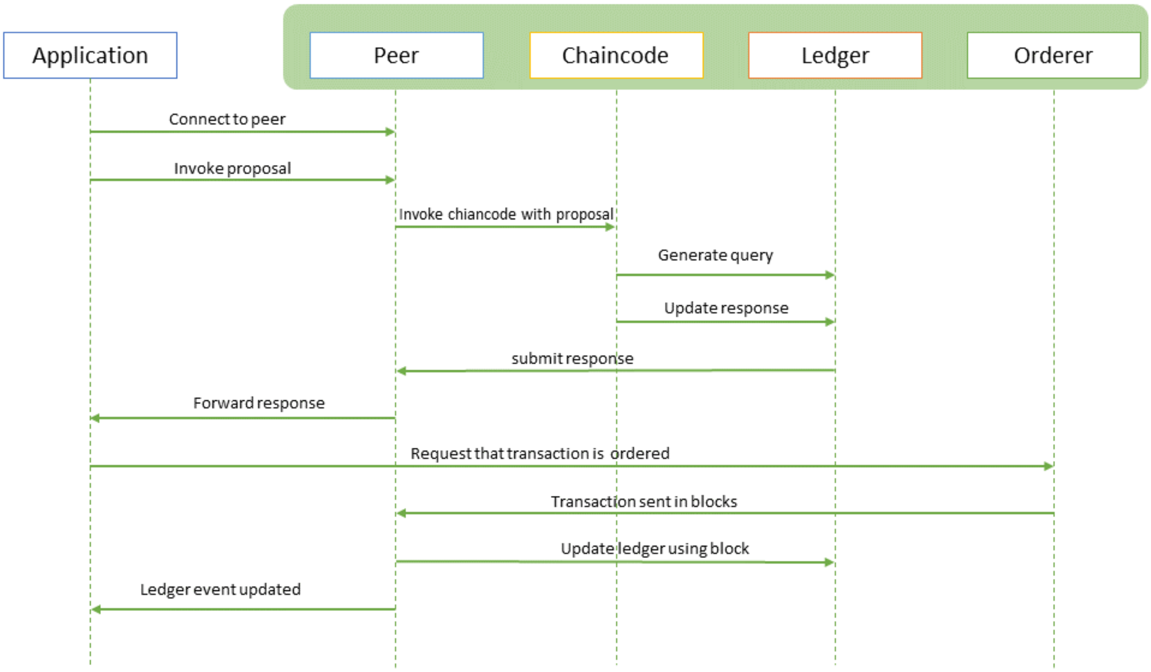


Figure 4. A sequence diagram of transaction processing.

3.1.4. Smart Contract

A smart contract is a computer program that can perform transactions and access blockchain blocks and records. It appends functionality to the blockchain. A smart contract is stored in a distributed database [44]. A smart contract allows the organization to enforce the desired limitation or validation upon transactions. Different rules and business logic are also coded in smart contracts. It can be viewed as a real-life example of an agreement between two parties. Both parties define some set of rules for the transaction of goods or services. But in a smart contract, these rules are enforced automatically with the help of computer code. Computer code for smart contracts contains parts for opening the deal, performing actions, and exiting. Figure 5 shows the system diagram of the smart contract and its communication with peer nodes. The input parameters determine the new world state. The response contains all the values of the world state as an RW-set.

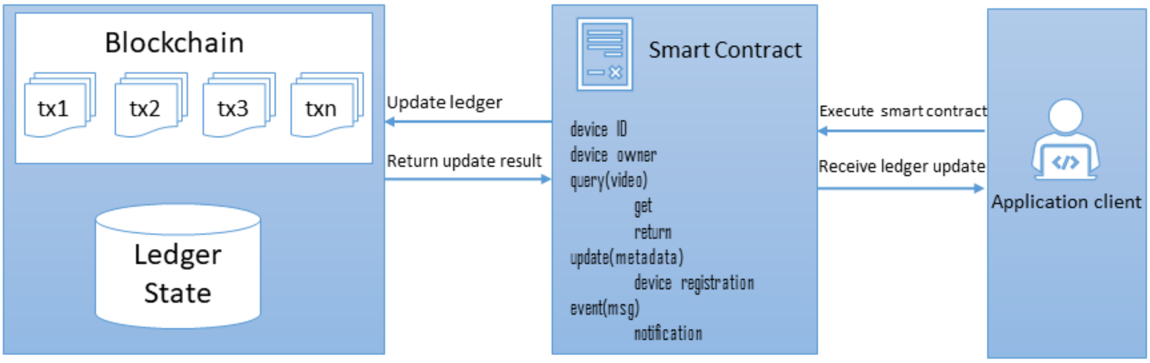


Figure 5. Smart contract for a CCTV–blockchain interaction.

The pseudo-code used for the operation of smart contracts is detailed in Algorithm 1. In this algorithm, a user requests a particular action. The access function is used to check whether the user can have access to $cctv_i$. It specifies whether that the user is authenticated to use the data generated by $cctv_i$.

Algorithm 1 Smart contract algorithm for granting access for a particular user request.

```
function access($cctv_i$)
Input :query($cctv_i$)
Output :granted, denied
if message ($cctv_i$) exists & query ($cctv_i$) is valid then
    check $cctv_i$ is granted/denied
    if $cctv_i$ is registered in the granted list then
        check role of $user_{id}$
        if $role =$ access then
            return granted
        else
            return denied
        end if
    else
        return denied
    end if
else
    return denied
end if
end function
```

3.2. Blockchain-Based Secure Data Sharing

The Blockchain-User Interaction Model represented in Figure 6 introduces three significant layers—the application, data, and sensor layers; the application layer consists of the user applications run by the clients and network administrators. Users can push and retrieve data using web browsers or client applications. The exchange of data occurs on the middle layer, which consists of the blockchain. This distributed ledger acts as a point of authentication and verification for the data and metadata of surveillance cameras. Different rules and smart contracts also run on this layer. These rules need to be developed in harmony with users, regulatory authorities, and infrastructure providers. Smart contract-based obligations, e.g., transactions of data and physical assets, can, therefore, be settled due to mutual trust in the blockchain. The sensor layer contains the image sensors or surveillance devices, which, in our case, are CCTV cameras.

Blockchain is the backbone of the proposed system. It functions without the need for intermediaries due its peer-to-peer and smart contract capabilities [45]. Further, trust among stakeholders is not a requirement because distributed ledger platform technology offers encryption features and complete traceability of every block.

3.3. Proposed CCTV Image Forgery and Alteration Verification Technique

The proposed system develops a blockchain interface among CCTV nodes and participants. Some frames of the image are selected and distributed through the blockchain network for image forgery and modulation verification. If all of the continuously created CCTV video frames are stored in the blockchain, the transaction of the blockchain becomes too large, which reduces the data size and increases the possibility of practical use by using only a few frames of every video. Some frames are verified to determine if the image is forged.

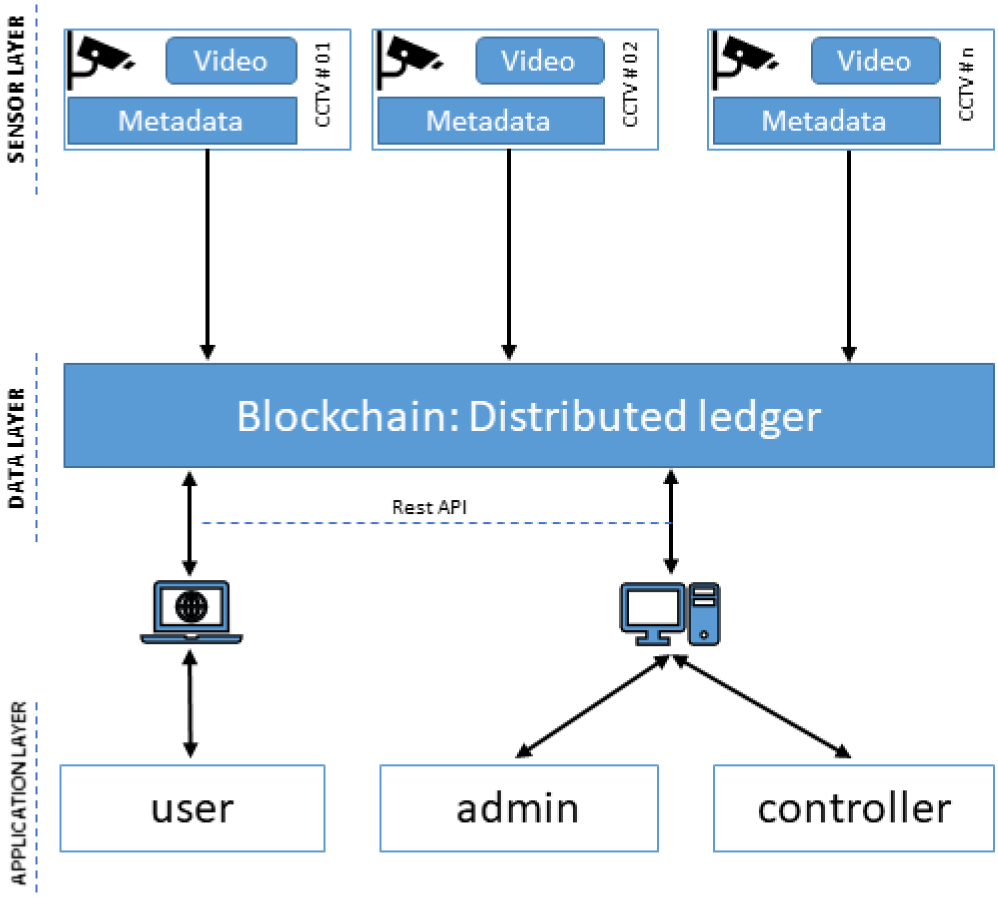


Figure 6. Blockchain-user interaction model.

3.3.1. Operation Flow

In a smart city, there could be n number of surveillance devices that interact with the IP video server. The control room manages the addition of new devices [46]. User applications act as a point of interaction with those devices and the blockchain. Image sensors send the sensor data and metadata to the blockchain through its communication interface. The number of frames per second to be extracted is determined according to the policy. If the importance is high, the number of frames per second is increased. Otherwise, only one frame per second is extracted to reduce the transaction size of the blockchain. It constructs block headers for extracted frames; adds CCTV IP and video generation time; performs digital signature with hashing, encryption, and a private key; and distributes generated blocks to the blockchain network. Participating nodes validate the validity of the received blocks and prove their work; and if successful, chain them and store them in a database.

Figure 7 shows the process of verification of image falsification and authentic surveillance node. The node that wants to verify the forgery and alteration of a CCTV image extracts the desired time zone block, and hashes, decodes, and signs to remove the frame. It verifies the forgery by comparing the frame of the image with the extracted frame. If it is the same, the image is not forged or altered. The user registers a new surveillance node on the blockchain through the IP video server. Before adding any modern device, it sends enrollment requests to the blockchain. The membership service provider (MSP) is responsible for issuing a private key to every user. It also sends an event notified after issuing the enrollment certificate. An enrolled user can generate a task through an IP video server. Every CCTV device is connected to the blockchain with the unique hashed key value. Every node sends the periodic metadata to store on the blockchain along with the video and image data. In a blockchain network, there are validating nodes that are specified by the network admin while configuring the system. Each block needs to be endorsed by an authenticating peer before being added into the chain.

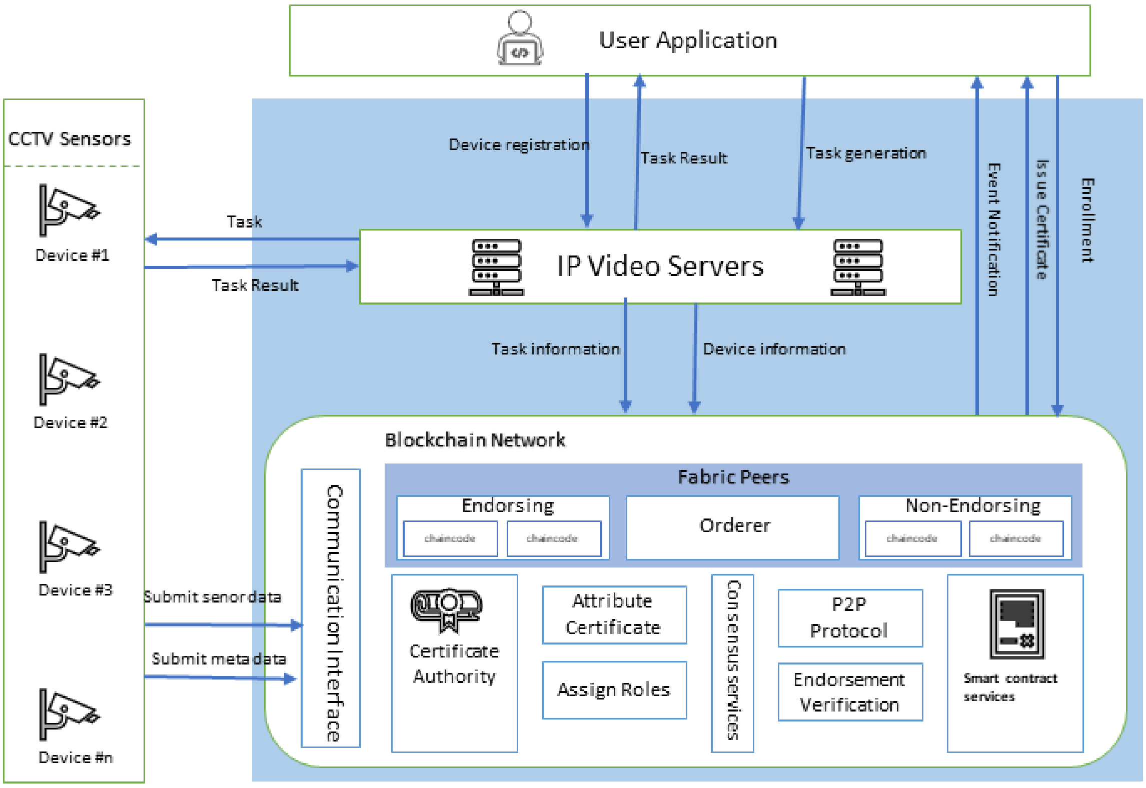


Figure 7. System model of the proposed CCTV-Blockchain platform.

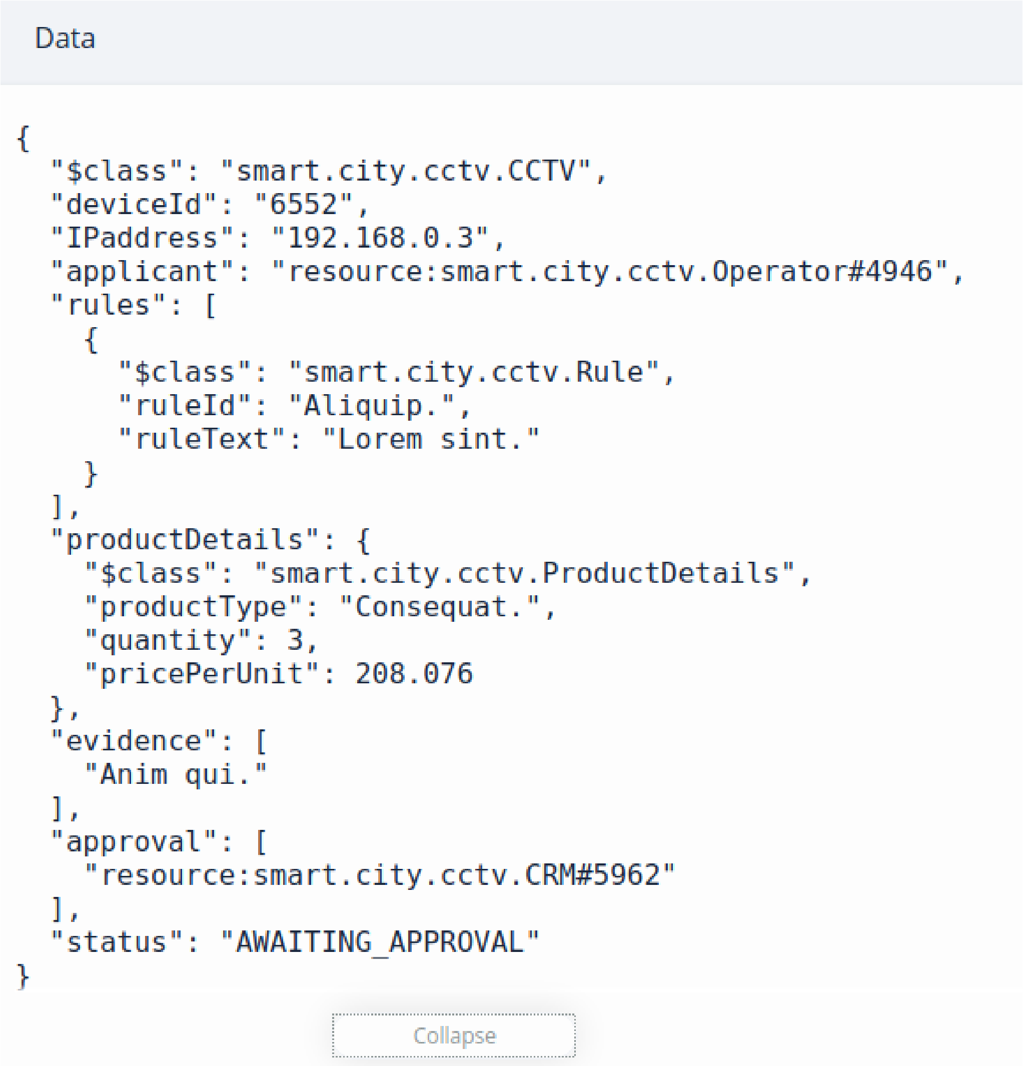
4. Results

In this section, we present a developmental evaluation of the proposed scheme using Hyperledger Fabric Composer Playground, and the results. The simulation environment used for implementation is summarized in Table 2. We have used Ubuntu 18.04.4 LTS operating system on Intel(R) Core(TM) i5-8500 with 16 GB RAM. Version 1.4 of the open-source framework Hyperledger Fabric is used to take full advantage of the latest updates. Composer Playground of Hyper Ledger is used as a development and testing tool, which gives an environment that quickly designs and examines a custom blockchain interface. The Command-line interface CLI composer tool of web-playground is used for the coding of business network definitions.

Table 2. CCTV-blockchain simulation environment.

Sr #	Component	Description
1	Processor	Intel(R) Core(TM) i5-8500
2	RAM	16 GB
3	OS	Ubuntu 18.04.4 LTS
4	Hyperledger Fabric	v 1.4
5	CLI	Composer-cli
6	IDE	Hyperledger Composer Playground

Our main focus is on CCTV cameras in smart cities, so we have used CCTV as an asset for our proposed system. The operator can add new assets in the system after the approval of control room manager. He can define the rules and product details while submitting the request for adding of new device. He also has to define the IP address of a camera. Figure 8 shows randomly generated data for a newly added asset.



```
{
  "$class": "smart.city.cctv.CCTV",
  "deviceId": "6552",
  "IPaddress": "192.168.0.3",
  "applicant": "resource:smart.city.cctv.Operator#4946",
  "rules": [
    {
      "$class": "smart.city.cctv.Rule",
      "ruleId": "Aliquip.",
      "ruleText": "Lorem sint."
    }
  ],
  "productDetails": {
    "$class": "smart.city.cctv.ProductDetails",
    "productType": "Consequat.",
    "quantity": 3,
    "pricePerUnit": 208.076
  },
  "evidence": [
    "Anim qui."
  ],
  "approval": [
    "resource:smart.city.cctv.CRM#5962"
  ],
  "status": "AWAITING_APPROVAL"
}
```

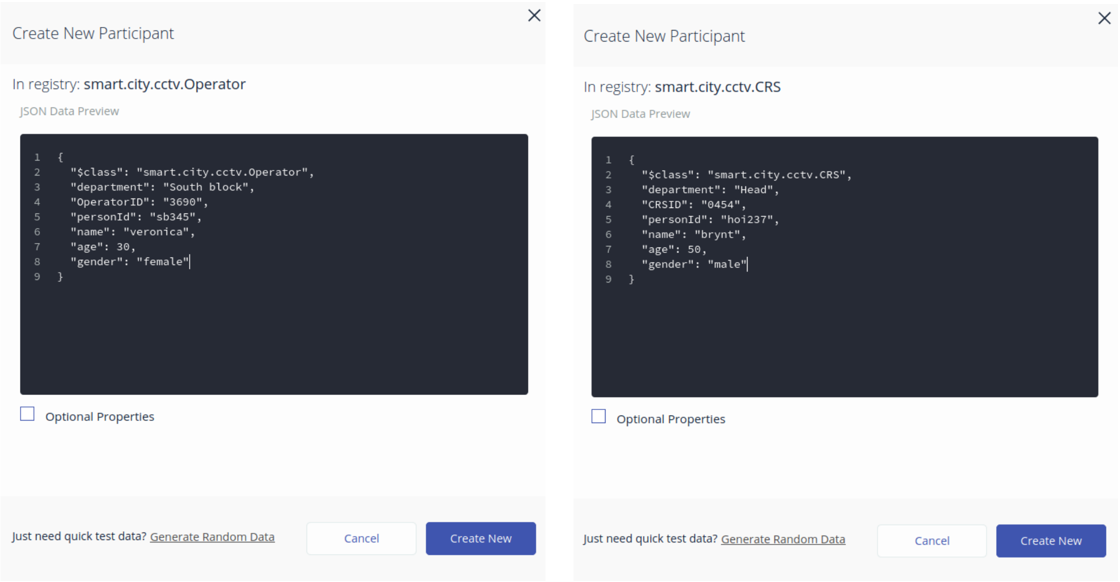
Figure 8. Meta Data for a CCTV device.

4.1. Participants

Participants are the members of the proposed system. They have their specific jobs and access controls according to the jobs [47]. Every participant of the blockchain network can initiate a transaction based on assets. They run the business network of the private blockchain. Table 3 shows the participants and their job descriptions. Instead of using full name, we have used the abbreviations of participants while writing the code and smart contracts. The proposed system consist of six participant types: the control room manager (CRM), control room supervisors (CRS), operators, police officers (POs), police control room operators (PCROs), and local authority staff (LAS). Figure 9 shows the interface to add new participants. The CRM ensures that all CCTV operators and team leaders are operating all equipment and cameras. The CRS operates all equipment and cameras in line with the CCTV control room policies. Operators perform two types of surveillance, proactive and reactive surveillance; they also do the CCTV video review and administration. POs use police radios to contact CCTV control room operators for incident support using CCTV cameras. PCROs contact the CCTV control room operators for reporting suspicious and actual incidents onsite. LAS use police radios to contact CCTV control room operators.

Table 3. Participants along with their job descriptions.

Sr #	Abbreviation	Participant	Job Description
1	CRM	Control Room Manager	Make sure that operators operate all devices and cameras
2	CRS	Control Room Supervisors	Manage all devices and CCTV cameras in line with the CCTV control room policies
3	Operator	Operator	Perform proactive and reactive surveillance
4	PO	Police Officers	Manage police radios to communicate CCTV command room operatives concerning event assistance utilizing CCTV
5	PCRO	Police Control Room Operators	Communicate CCTV command room operatives concerning communicating suspicious events onsite
6	LAS	Local Authority Staff	Manage police radios to communicate CCTV command room operatives


Create New Participant
×
In registry: smart.city.cctv.Operator
JSON Data Preview

```
{
  "$class": "smart.city.cctv.Operator",
  "department": "South block",
  "OperatorID": "3690",
  "personId": "sb345",
  "name": "veronica",
  "age": 30,
  "gender": "female"
}
```

□ Optional Properties
Just need quick test data? Generate Random Data
Cancel
Create New

(**a**) Operator

Create New Participant
×
In registry: smart.city.cctv.CRS
JSON Data Preview

```
{
  "$class": "smart.city.cctv.CRS",
  "department": "Head",
  "CRSID": "0454",
  "personId": "hoi237",
  "name": "brynt",
  "age": 50,
  "gender": "male"
}
```

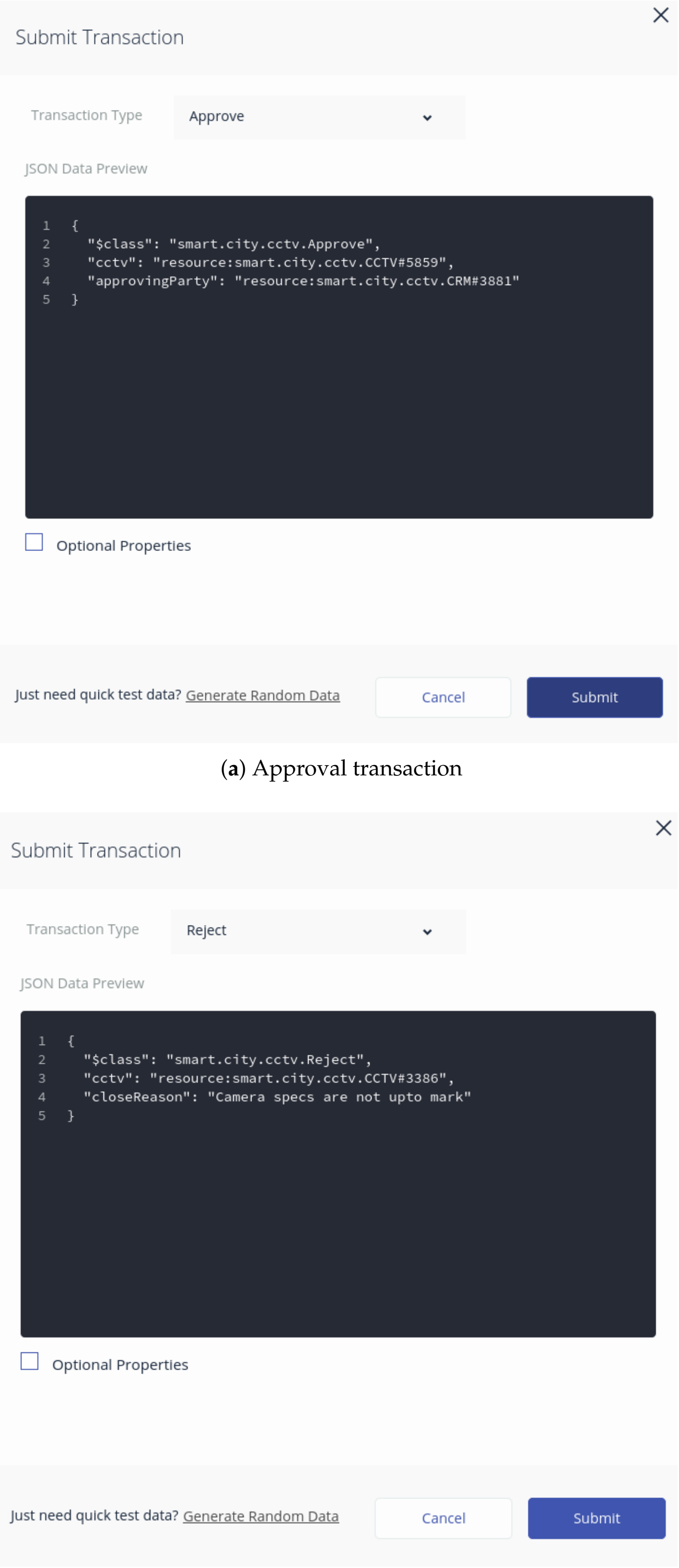
□ Optional Properties
Just need quick test data? Generate Random Data
Cancel
Create New

(**b**) CRS

Figure 9. Add new participants.

4.2. Transaction

Every certified participant of the proposed network can start a new transaction based on the rules defined in smart contracts. After successfully executing the transaction, smart contracts generate a response to the participant. Figure 10 shows two types of transactions. Figure 10a shows a transaction to approve the addition of a new device by the CRM, and Figure 10b shows a rejection by the CRM.



Submit Transaction

Transaction Type: Approve

JSON Data Preview

```
{
  "$class": "smart.city.cctv.Approve",
  "cctv": "resource:smart.city.cctv.CCTV#5859",
  "approvingParty": "resource:smart.city.cctv.CRM#3881"
}
```

□ Optional Properties

Just need quick test data? Generate Random Data

(**a**) Approval transaction

Submit Transaction

Transaction Type: Reject

JSON Data Preview

```
{
  "$class": "smart.city.cctv.Reject",
  "cctv": "resource:smart.city.cctv.CCTV#3386",
  "closeReason": "Camera specs are not upto mark"
}
```

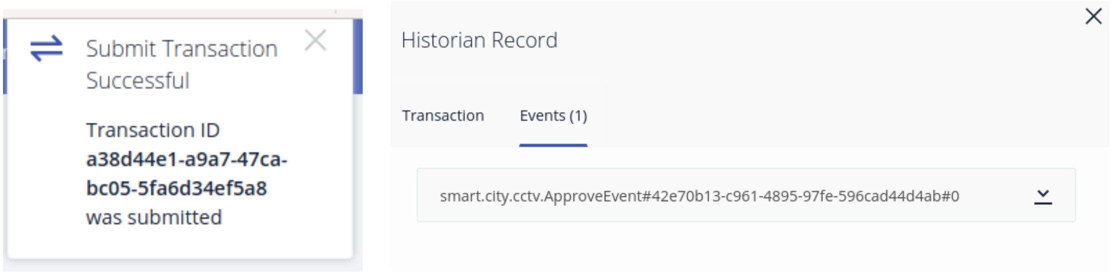
□ Optional Properties

Just need quick test data? Generate Random Data

(**b**) Rejection transaction

Figure 10. Submitting new transactions.

On successful completion of the transaction, a notification (Figure 11a) and a unique event ID (Figure 11b) are generated.



Submit Transaction Successful

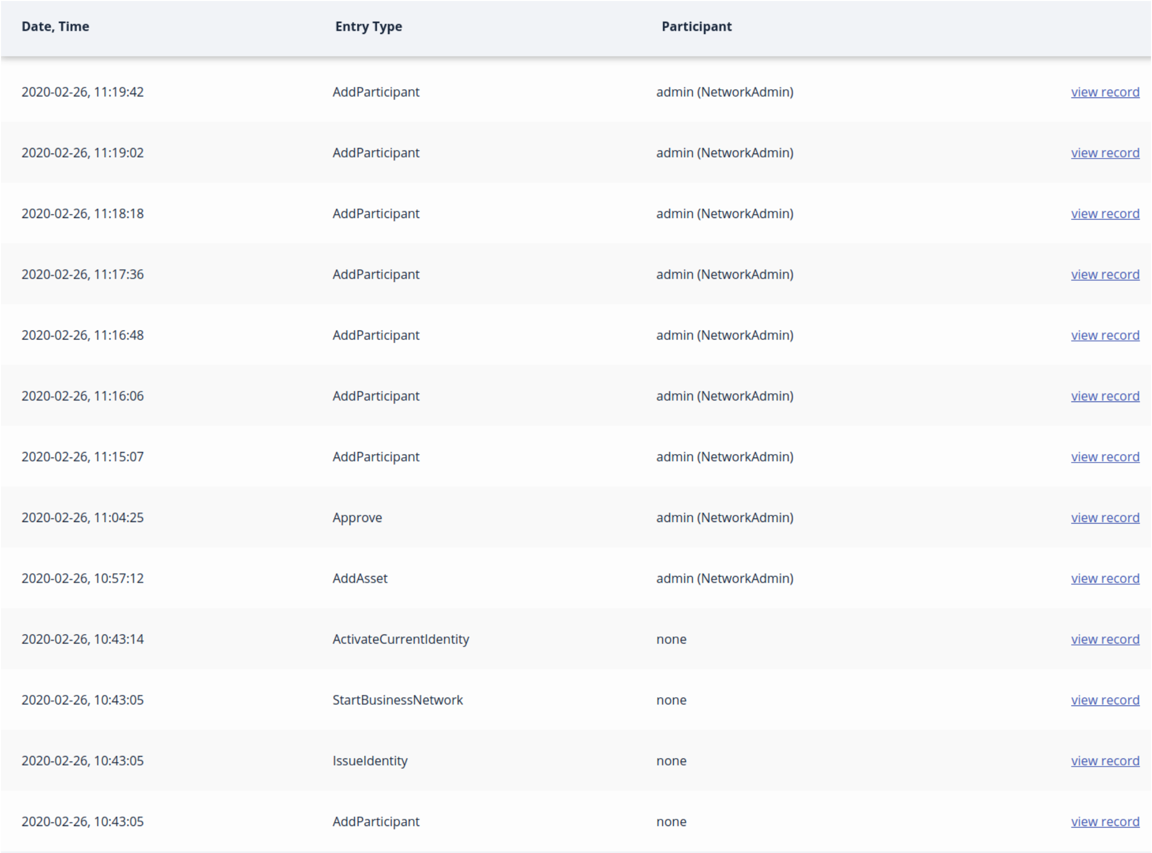
Transaction ID a38d44e1-a9a7-47ca-bc05-5fa6d34ef5a8 was submitted

smart.city.cctv.ApproveEvent#42e70b13-c961-4895-97fe-596cad44d4ab#0

(**a**) Event notification (**b**) Event ID

Figure 11. Notification upon successful transaction submission.

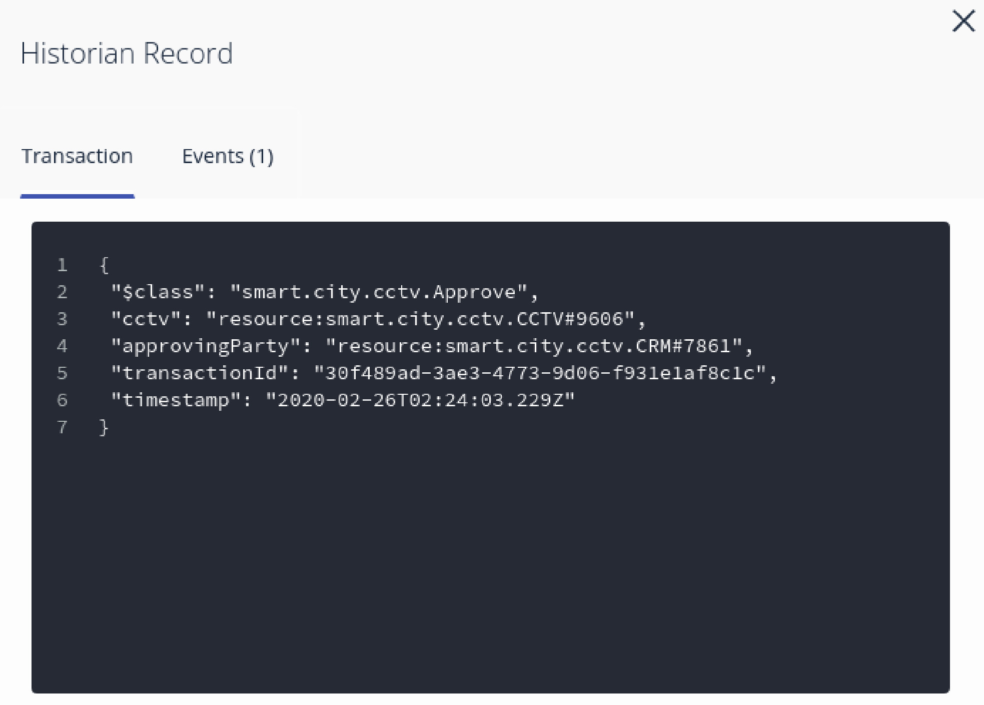
We can see all the transactions with immutable dates, times, entry types and participants in Figure 12.



Date, Time	Entry Type	Participant	
2020-02-26, 11:19:42	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:19:02	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:18:18	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:17:36	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:16:48	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:16:06	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:15:07	AddParticipant	admin (NetworkAdmin)	view record
2020-02-26, 11:04:25	Approve	admin (NetworkAdmin)	view record
2020-02-26, 10:57:12	AddAsset	admin (NetworkAdmin)	view record
2020-02-26, 10:43:14	ActivateCurrentIdentity	none	view record
2020-02-26, 10:43:05	StartBusinessNetwork	none	view record
2020-02-26, 10:43:05	IssueIdentity	none	view record
2020-02-26, 10:43:05	AddParticipant	none	view record

Figure 12. Transaction list.

We can also see each transaction's details with immutable date and unique event ID (Figure 13).

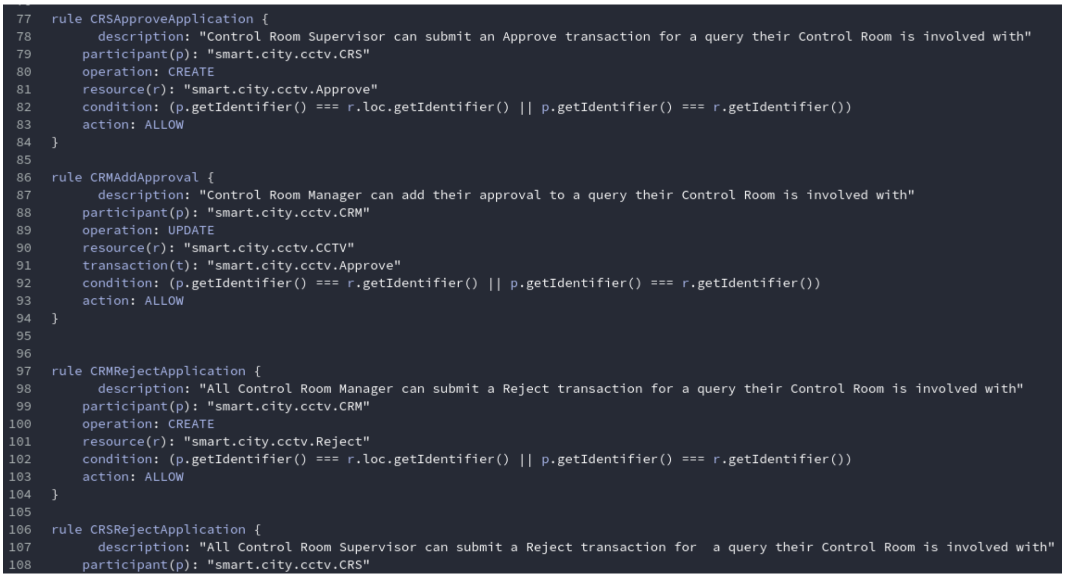


```
{
 "$class": "smart.city.cctv.Approve",
 "cctv": "resource:smart.city.cctv.CCTV#9606",
 "approvingParty": "resource:smart.city.cctv.CRM#7861",
 "transactionId": "30f489ad-3ae3-4773-9d06-f931e1af8c1c",
 "timestamp": "2020-02-26T02:24:03.229Z"
}
```

Figure 13. Record of transaction history.

4.3. Smart Contract Implementation

There are four segments within a smart contract of hyperledger; i.e., model, query definition, script, and access control rules. Hyperledger Fabric supports the adoption of state databases based on the format of the data amongst LevelDB and CouchDB. These two databases back core chaincode transactions. LevelDB is the default state database that is implemented to conserve smart contract data as a key-value pair. It is embedded in the peer node of the system. The alternative to LevelDB is CouchDB, which is used to format data of chaincode as binary code. It also concedes fitting the reporting demands. Transaction processor roles are inscribed in JavaScript and confined in a separate file as a part of a smart contract definition. Figure 14 shows a snippet of smart contract rules.



```
rule CRSApproveApplication {
      description: "Control Room Supervisor can submit an Approve transaction for a query their Control Room is involved with"
    participant(p): "smart.city.cctv.CRS"
    operation: CREATE
    resource(r): "smart.city.cctv.Approve"
    condition: (p.getIdentifier() === r.loc.getIdentifier() || p.getIdentifier() === r.getIdentifier())
    action: ALLOW
}

rule CRMAddApproval {
      description: "Control Room Manager can add their approval to a query their Control Room is involved with"
    participant(p): "smart.city.cctv.CRM"
    operation: UPDATE
    resource(r): "smart.city.cctv.CCTV"
    transaction(t): "smart.city.cctv.Approve"
    condition: (p.getIdentifier() === r.getIdentifier() || p.getIdentifier() === r.getIdentifier())
    action: ALLOW
}


rule CRMRejectApplication {
      description: "All Control Room Manager can submit a Reject transaction for a query their Control Room is involved with"
    participant(p): "smart.city.cctv.CRM"
    operation: CREATE
    resource(r): "smart.city.cctv.Reject"
    condition: (p.getIdentifier() === r.loc.getIdentifier() || p.getIdentifier() === r.getIdentifier())
    action: ALLOW
}

rule CRSRejectApplication {
      description: "All Control Room Supervisor can submit a Reject transaction for  a query their Control Room is involved with"
    participant(p): "smart.city.cctv.CRS"
```

Figure 14. Transaction control rules in the smart contract.

4.4. *Cost-Benefit Analysis*

The cost-benefit analysis includes the steps involved in the decision-making about the feasibility of a system. The market for smart city surveillance equipment is increasing day by day. According to [48], this could reach up to 19.5 billion Euros by the year 2023. As per the data gathered from [49], the largest market for surveillance equipment is Asia, and more specifically, China. Out of the top 10 most-surveilled cities in the world, eight are in China. Figure 15 shows the top 10 cities around the world according to the number of cameras, and it also indicates the safety indexes of those cities. EL Piza and his associates [50] conducted a study in 2019. Their study was based on 40 years of evaluation research. They found out that CCTV is the most effective technology to reduce crimes in residential areas and car parks. That is why this technology is worth spending money on—the safety of people in cities.

There are mainly three types of costs in such a system: purchasing, personnel, and running. Purchasing cost is a one time cost, and usually, it is the most significant portion of the entire system cost. It includes the purchase of initial hardware and setup cost. Personnel costs consist of the salaries of the staff, such as the POs and CRM. It is a continuous cost to run the system effectively. Running costs include the maintenance costs, which can vary according to the life of the hardware. Our proposed approach is using an open-source blockchain technology, which will help in security issues related to CCTV camera recordings. It will also reduce the centralized storage and maintenance costs, as blockchain provides a distributed environment with the guaranty of immutability, security, and privacy.

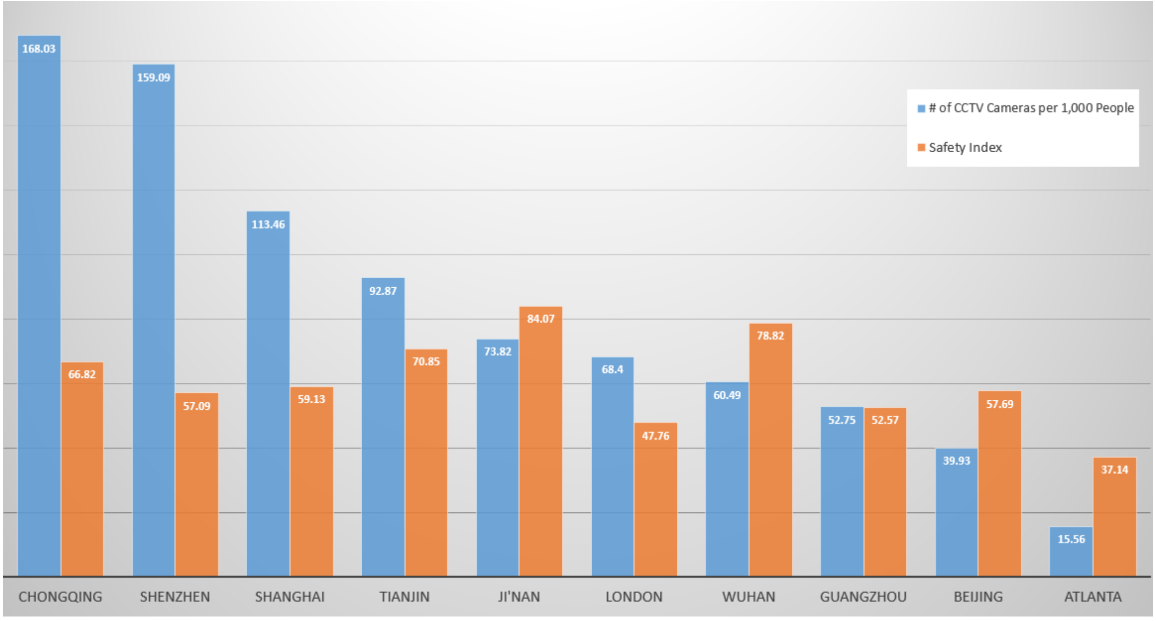


Figure 15. Top 10 cities according to the number of surveillance cameras.

5. Discussion

A smart city is an urban environment where people enjoy a safe and secure life. Safety is one of the significant factors to keep in mind for the decision-makers of a smart city. Blockchain technology is widely used in many areas of smart cities, including smart grids, smart hospitals, smart vehicles, and supply chains. We first discussed blockchain and CCTV cameras and examined the overview of surveillance environment and blockchain-based video. We looked at research trends on surveillance. One of the major flaws we found in the current research is the verification of data. Data from surveillance cameras can be used as evidence in the court, but to ensure that the evidence is not forged is a problem. The market for surveillance cameras is increasing as countries are trying to provide safe environments to their people. Chongqing, a populous city in China, is the most surveilled city in the world, where there are around 168 cameras per 1000 citizens. China is planning to increase the number up to one camera per two persons [51]. This will inevitably produce a large amount of metadata along with digital videos. The increasing number of imaging sensors for surveillance also opens a window for potential security attacks. The current systems are vulnerable to physical attacks. The user data is at risk of misuse. Hence, there was a gap in the research regarding a secure and trusted network. The authentication of surveillance devices also needs a trusted mechanism to be enlisted in the system. In this paper, A robust security platform based on blockchain technology is designed and applied. The high-security blockchain technology is applied to CCTV security data of a smart city. The blockchain is a trusted platform; hence, it can be used to deal with the legal aspects regarding the authenticity of the evidence. Reference [20] gives a solution to data integrity management of the supply chain using blockchain. In their work, they explained the use of Hyperledger Fabric in detail to ensure data safety in the smart hospital. Hyperledger Fabric is an open-source platform by Linux foundation which provides hashed signatures to every participant and every node. Transactions within the blockchain are encrypted and timestamped. A block within this system is immutable, and nobody can change the timestamped data. Blocks are even verified before adding to the security chain. Hack-proof algorithms of blockchains provide trust to the consumers and decision-makers. We offer a system using a private blockchain; hence, it adds one more layer of security. In a private blockchain, every participant needs a private key through the MSP. Only legitimate operators can use the data.

Another point that can be helpful in legal issues is the metadata saved using the smart contract, which includes the IP address of data-generating devices and participants who are dealing with the device. The blockchain also provides data integrity, which ensures that the stored data does not get tampered with. The proposed solution is a cost-effective way to authenticate data for surveillance cameras. Another critical aspect of the proposed method is its decentralization, which will be helpful in fault tolerance. The data is distributed in different nodes; hence, in case of any failure in any node, the data can be retrieved easily. This research will help in the reshaping of better and secure smart cities. The proposed scheme allows the interested parties to go through the implementation details of a secured system.

6. Conclusions

The concepts underlying smart cities and surveillance technologies are strongly interconnected. CCTV video security technology is concerned with personal privacy. Blockchain technology is a modern-day solution to integrity and security problems. Blockchain technology is suitable for this purpose because it can guarantee safety from the manipulation of data, and also ideal for the safe storage of image information through a distributed ledger. One remaining aspect to reflect upon consists of the problem regarding a large bandwidth and incentive mechanism, which can be addressed in future research.

Author Contributions: Conceptualization, P.W.K.; Formal analysis, P.W.K.; Funding acquisition, Y.-C.B.; Investigation, N.P.; Methodology, P.W.K.; Project administration, Y.-C.B.; Supervision, Y.-C.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response]. And, this work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374)

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the design of this study, the analyses, or the writing of this manuscript.

Abbreviations

The following abbreviations are used in this manuscript:

CCTV	closed-circuit television camera
IoT	Internet of Things
AI	artificial intelligence
KRW	South Korean Won
RW-set	read write set
MSP	membership service provider
IP	Internet protocol
CLI	command-line interface
CRM	control room manager
CRS	control room supervisor
PO	police officer
PCRO	police control room operator
LAS	local authority staff

References

1. Talari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P. A review of smart cities based on the internet of things concept. *Energies* **2017**, *10*, 421. [CrossRef]
2. Wu, T.Y.; Fan, X.; Wang, K.H.; Lai, C.F.; Xiong, N.; Wu, J.M.T. A DNA Computation-Based Image Encryption Scheme for Cloud CCTV Systems. *IEEE Access* **2019**, *7*, 181434–181443. [CrossRef]
3. Li, Y.; Lyu, S. Exposing deepfake videos by detecting face warping artifacts. *arXiv* **2018**, arXiv:1811.00656.
4. Ravi, H.; Subramanyam, A.V.; Gupta, G.; Kumar, B.A. Compression noise based video forgery detection. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014; pp. 5352–5356.
5. Hasan, H.R.; Salah, K. Combating deepfake videos using blockchain and smart contracts. *IEEE Access* **2019**, *7*, 41596–41606. [CrossRef]
6. Shen, M.; Deng, Y.; Zhu, L.; Du, X.; Guizani, N. Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach. *IEEE Netw.* **2019**, *33*, 27–33. [CrossRef]
7. Khan, P.W.; Byun, Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. *Entropy* **2020**, *22*, 175. [CrossRef]
8. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, *89*, 746–764. [CrossRef]
9. Gipp, B.; Kosti, J.; Breitinger, C. *Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain*; MCIS: Selangor, Malaysia, 2016; p. 51.
10. Lee, J.H. BIDaaS: Blockchain based ID as a service. *IEEE Access* **2017**, *6*, 2274–2278. [CrossRef]
11. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
12. Hashemi, S.H.; Faghri, F.; Campbell, R.H. Decentralized user-centric access control using pubsub over blockchain. *arXiv* **2017**, arXiv:1710.00110.
13. Kiyomoto, S.; Rahman, M.S.; Basu, A. On blockchain-based anonymized dataset distribution platform. In Proceedings of the 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, UK, 7–9 June 2017; pp. 85–92.
14. Danzi, P.; Angjelichinoski, M.; Stefanović, Č.; Popovski, P. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 45–51.
15. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
16. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed Blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **2017**, *13*.

17. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedings of the 2017 International conference on service systems and service management, Dalian, China, 16–18 June 2017; pp. 1–6.
18. Herbaut, N.; Negru, N. A model for collaborative blockchain-based video delivery relying on advanced network services chains. *IEEE Commun. Mag.* **2017**, *55*, 70–76. [CrossRef]
19. Yavuz, E.; Koç, A.K.; Çabuk, U.C.; Dalkılıç, G. Towards secure e-voting using ethereum blockchain. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–7.
20. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics* **2019**, *8*, 505. [CrossRef]
21. Gretzel, U.; Werthner, H.; Koo, C.; Lamsfus, C. Conceptual foundations for understanding smart tourism ecosystems. *Comput. Hum. Behav.* **2015**, *50*, 558–563. [CrossRef]
22. Javaid, U.; Siang, A.K.; Aman, M.N.; Sikdar, B. Mitigating loT device based DDoS attacks using blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 10–15 June 2018; pp. 71–76.
23. Kim, S.K.; Kim, U.M.; Huh, J.H. A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. *Energies* **2019**, *12*, 402. [CrossRef]
24. Hang, L.; Kim, D.H. Reliable Task Management Based on a Smart Contract for Runtime Verification of Sensing and Actuating Tasks in IoT Environments. *Sensors* **2020**, *20*, 1207. [CrossRef]
25. D'Avino, D.; Cozzolino, D.; Poggi, G.; Verdoliva, L. Autoencoder with recurrent neural networks for video forgery detection. *Electron. Imaging* **2017**, *2017*, 92–99. [CrossRef]
26. Sulaiman, N.; Bagiwa, M.A.; Aliyu, S.; Shafii, K.; Usman, A.M.; Mohammed, S.; Abdulsalam, A.J. DETECTION AND LOCALIZATION OF SPLICING FORGERY IN DIGITAL VIDEOS USING CONVOLUTIONAL AUTO-ENCODER AND GOTURN ALGORITHM. *FUDMA J. Sci.* **2019**, *3*, 449–458.
27. Zhang, W.; Liu, Y.; Das, S.K.; De, P. Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. *Pervasive Mob. Comput.* **2008**, *4*, 658–680. [CrossRef]
28. Sowmya, K.; Chennamma, H.; Rangarajan, L. Video authentication using spatio temporal relationship for tampering detection. *J. Inf. Secur. Appl.* **2018**, *41*, 159–169.
29. Hsu, C.C.; Hung, T.Y.; Lin, C.W.; Hsu, C.T. Video forgery detection using correlation of noise residue. In Proceedings of the 2008 IEEE 10th Workshop on Multimedia Signal Processing, Cairns, Australia, 8–10 October 2008; pp. 170–174.
30. Song, J.; Yang, Y.; Huang, Z.; Shen, H.T.; Luo, J. Effective multiple feature hashing for large-scale near-duplicate video retrieval. *IEEE Trans. Multimed.* **2013**, *15*, 1997–2008. [CrossRef]
31. Nassauer, A. How robberies succeed or fail: Analyzing crime caught on CCTV. *J. Res. Crime Delinq.* **2018**, *55*, 125–154. [CrossRef]
32. Kwon, B.W.; Sharma, P.K.; Park, J.H. CCTV-Based Multi-Factor Authentication System. *J. Inf. Process. Syst.* **2019**, *15*, 904–919.
33. Panwar, N.; Sharma, S.; Wang, G.; Mehrotra, S.; Venkatasubramanian, N.; Diallo, M.H.; Sani, A.A. IoT Notary: Sensor data attestation in smart environment. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28, September 2019; pp. 1–9.
34. Qayyum, A.; Qadir, J.; Janjua, M.U.; Sher, F. Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News. *IT Prof.* **2019**, *21*, 16–24. [CrossRef]
35. Ghimire, S.; Choi, J.Y.; Lee, B. Using Blockchain for Improved Video Integrity Verification. *IEEE Trans. Multimed.* **2019**, *22*, 108–121. [CrossRef]
36. Kerr, M.; Han, F.; van Schyndel, R. A blockchain implementation for the cataloguing of cctv video evidence. In Proceedings of the 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018; pp. 1–6.
37. Karame, G. On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1861–1862.
38. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]

39. Cachin, C.; others. Architecture of the hyperledger blockchain fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25 July 2016; Volume 310, p. 4.
40. Lai, K. Blockchain as AML tool: A work in progress. *Int. Financ. Law Rev.* **2018**. Available online: https://www.iflr.com/Article/3804315/Blockchain-as-AML-tool-a-work-in-progress.html?ArticleId=3804315 (accessed on 10 March 2020)
41. Decker, C.; Wattenhofer, R. Information propagation in the bitcoin network. In Proceedings of the IEEE P2P 2013 Proceedings, Trento, Italy, 9–11 September 2013; pp. 1–10.
42. Gupta, S.; Sadoghi, M. Blockchain Transaction Processing. In *Encyclopedia of Big Data Technologies*; Springer International Publishing: Cham, Switzerland, 2019. .
43. Zhang, S.; Zhou, E.; Pi, B.; Sun, J.; Yamashita, K.; Nomura, Y. A Solution for the Risk of Non-deterministic Transactions in Hyperledger Fabric. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 253–261.
44. Hang, L.; Kim, D.H. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228. [CrossRef]
45. Kamilaris, A.; Fonts, A.; Prenafeta-Boldΰ, F.X. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci. Technol.* **2019**, *91*, 640–652. [CrossRef]
46. Bang, J.; Lee, Y.; Lee, Y.T.; Park, W. AR/VR Based Smart Policing For Fast Response to Crimes in Safe City. In Proceedings of the 2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), Beijing, China, 10–18 October 2019; pp. 470–475.
47. Sajana, P.; Sindhu, M.; Sethumadhavan, M. On blockchain applications: Hyperledger fabric and ethereum. *Int. J. Pure Appl. Math.* **2018**, *118*, 2965–2970.
48. Cities Going Big on Surveillance Tech. 2020. Available online: https://www.smartcitiesworld.net/news/news/cities-going-big-on-surveillance-tech-4913 (accessed on 10 March 2020).
49. Surveillance camera statistics: Which cities have the most CCTV cameras? 2020. Available online: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (accessed on 10 March 2020).
50. Piza, E.L.; Welsh, B.C.; Farrington, D.P.; Thomas, A.L. CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminol. Public Policy* **2019**, *18*, 135–159. [CrossRef]
51. China will have 'one street camera for every TWO PEOPLE. 2020. Available online: https://www.dailymail.co.uk/news/article-7379255/China-one-CCTV-camera-TWO-PEOPLE-year.html (accessed on 10 March 2020).