Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 3, No. 3, 2025, Pages 173-193
DOI: 10.47831/mjpas.v3i3.326

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage*:*
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE - COMPUTER SCIENCE

Security surveillance systems based on deep learning and Blockchain techniques: a review

Maysam Majid Sabri [1*], Haider Kadhim Hoommod [2], Khalid Ali Hussein [3]

[1,2,3]Computer Science Department, College of Education, Mustansiriyah University

[*] Corresponding author E-mail: maysam_majid@uomustansiriyah.edu.iq

Article Info.

Article history:

Received
18 September 2024

Accepted
30 September 2024

Publishing
30 June 2025

Abstract

A building security surveillance system typically refers to a comprehensive setup designed to monitor and enhance security within a specific building. This system typically integrates various technologies and components to detect, assess, and respond to potential security threats. The ability of deep learning systems to draw informed conclusions has made them very popular in the field of security monitoring systems. However, centralized servers in many current deep learning systems prevent providing essential features such as verified data provenance, operational transparency, traceability, and reliability. On the other side, blockchain technology is a distributed and decentralized digital system composed of a series of blocks that include encrypted transaction data that can be shared among network users. Therefore, the integration of deep learning and blockchain technologies into security surveillance systems is an important area that provides improvements in data analysis, privacy, security, and overall efficiency of surveillance systems. This article reviews the significance of integrating deep learning algorithms and blockchain technology to develop a building security monitoring system. Furthermore, research related to integrating deep learning techniques with blockchain technology will be presented. Therefore, topics such as deep convolutional neural networks, blockchain concepts, and the measurements used to link these two technologies will be investigated and discussed. Finally, we present a comprehensive discussion of the state-of-the-art articles that must be investigated for building a robust deep learning system based on blockchain technology for security monitoring systems.

The official journal published by the College of Education at Mustansiriya University

Keywords*: Blockchain, CNN, deep learning, monitoring system ,AI,*

1. Introduction

Security and surveillance systems include various technologies and strategies designed to monitor, secure, and protect people, property, and information. These systems are used in residential, commercial, industrial, and government buildings. These systems are critical to protecting property and people, so they must be implemented carefully, taking into account the potential implications for privacy and the evolving nature of threats.Deep learning is a subset of artificial intelligence (AI). In computer science, deep learning refers to the training and application of artificial neural networks. The use of deep learning algorithms has shown significant results in numerous complex decision-making processes such as pattern, recognition, healthcare, language translation, and fraud detection due to its impressive precision results. Therefore, deep learning algorithms are used to solve different real-life problems (see Ref. [1]). Deep learning models may use facial recognition and biometric security features to detect physical threats[2]. The efficiency of a deep learning model is related to the quality of the data utilized in the stage of model training[3]. The majority of the deep learning models rely on centralized storage and processing which makes them sensitive to single points of failure and data manipulation by attackers. Any modification to the data in deep learning processes leads to damage to the training model. On the other side, blockchain is considered is decentralized technology, capable of effectively managing data security integrity, and confidentiality [4][5]. Blockchain technology continues to evolve and has the potential to completely change the way we handle data, automate payments, and track transactions. Blockchain technology can play a very cost-effective role in reducing the need for a central authority to control and verify transactions between participants. Every blockchain transaction is cryptographically signed and examined by all nodes that contain an exact copy of the ledger. The ledger contains complete information about all transactions in the system. Consequently, time-stamped, updated, and safe records are created that are unchangeable [6]. Blockchain technology and deep learning can be a powerful combination in various applications. The computer vision and machine learning sectors have paid close attention to the vast, varied, and complex field of deep comprehension and learning about human activities. Applications of deep learning extend to various areas, including but not restricted to computer vision, multimedia semantic annotations, indexing, and video monitoring [5][7][8][9]. Therefore, The combination of blockchain and deep learning offers various advantages, such as automated and trustworthy decision-making, effective management of data markets, enhanced data security, improved model construction for predictive purposes, facilitation of model sharing, enforce the resistance of deep learning-based models[10]. This area has attracted increased research attention and funding due to the growing demand for global security concerns and the increasing need for effective monitoring in both public and private places. Therefore, in such a situation the goal is to detect and identify interesting events that can be contextually defined as abnormal behavior[11][12]. Blockchain technology is capable of solving the problems associated with central data processing and storage. Blockchain is considered a promising technique that allows users in a decentralized network to keep a shared ledger of data. Blockchain ensures that every ledger copy maintained by participants is verified and has a consistent provenance [13]. By design, blockchain is a tamper-resistant and flexible technology that helps verify data to ensure it has not been distorted or altered [14][15]. Blockchain technology can source machine learning models that are created and trained by different systems. This enables to creation of robust Artificial Intelligence (AI) systems. Storing machine learning data on a blockchain network reduces the chances of errors occurring in the system because the blockchain network by its nature does not contain duplicate or missing data, which is essential for systems that rely on artificial intelligence [16]. The combination of deep learning with blockchain has significant promise in the realm of security and surveillance applications. Nevertheless, there are substantial obstacles to this amalgamation. To overcome these obstacles, it will be necessary to put in effort, develop new ideas, and thoroughly analyze the ethical, technical, and regulatory aspects. Effective and responsible utilization of these technologies requires collaboration among technologists, policymakers, and users. These problems emphasize the necessity of meticulous planning and thoughtful deliberation throughout the use of deep learning and blockchain technologies in security and surveillance systems. The combination of blockchain technologies and machine learning offers numerous significant advantages for applications, such as data management, data authenticity, audits, and the addition of new transactions to business processes through automation enabled by smart systems[17].

2. BACKGROUND

2.1 BLOCKCHAIN

Blockchain technology has become a very interesting field of study in the field of digital innovation, supporting a decentralized and secure framework for processing transactions and information. Blockchain was conceived as the underlying technology for the cryptocurrency Bitcoin, but it has since evolved into a versatile and impactful solution with applications across many other sectors[18][19]. The concept of blockchain was introduced in 2008 under the pseudonym Satoshi Nakamoto. The primary goal was to establish a decentralized and transparent system (like a bank) that could handle financial transactions without the need for a central authority. As a result, the first and the most well-known cryptocurrency, Bitcoin was introduced using blockchain technology as its underlying foundation[20]. Blockchain is a distributed digital system that represents a chain of blocks, including transaction data that can be shared in an encrypted format among the participants connected to the network. Blockchain is made up of several nodes that arrange transactions into blocks for recording and verifying transactions. Each block in the chain contains a group of transactions, and it is ensured that the newly created block is precisely connected to every other block in the chain to build an uninterrupted chain of blocks. Once the new block has joined its nearby chain, the recently added block is engineered to all participating hubs for assurance.

2.1.1 Theoretical Basis of Blockchain

Many ideas from distributed systems, cryptography, and computer science make up the theoretical foundation of blockchain technology [13], [21]. Blockchain technology operates on the concepts of distributed systems, wherein a network of nodes collaboratively exchange identical resources to accomplish a common objective. This method enhances the ability of the systems to resist errors and preserve functionality. Blockchain systems provide security and dependability required for modern digital transactions. Blockchain employs a highly secure software system that is very resistant to alteration. [22]. The system does not have a single point of failure, and individual users are unable to modify transaction records [17], (see Figure 1).

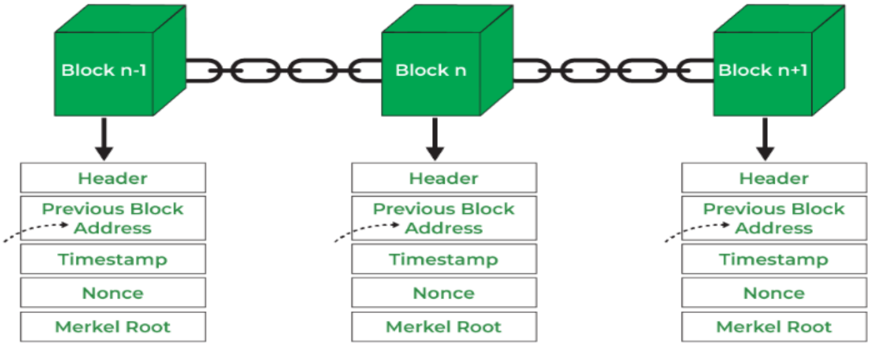


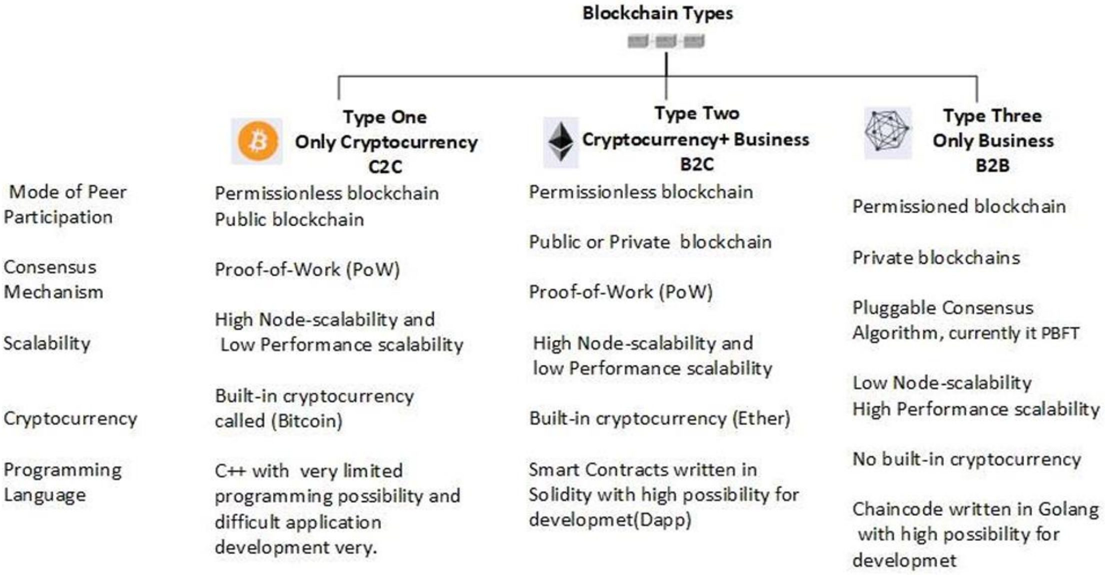
Figure 1: Blockchain diagram. Header: Identifies the block in the blockchain. Previous

Block Address/Hash: The hash connects the i+1th and ith blocks. Timestamp: The technique verifies data in blocks and assigns digital document creation dates. Nonce: It is key to the block's proof of work. Merkel Root: A data structure frame with several data blocks. Decentralized systems may find it easier to overcome the difficulties of reaching a unified conclusion with the help of consensus approaches. All of a network's nodes will agree on the validity of each transaction and its order if these techniques are used. Methods such as proof-of-stake, which selects valuators by the consensus mechanism of the blockchain network, and proof-of-work, which asks users to solve difficult mathematical problems, are the concepts that allow blockchain networks to reach agreements[23].

Companies utilize smart contracts to autonomously execute contractual agreements without requiring an intermediary. They are automated programs stored on the blockchain system that execute when specific conditions are fulfilled. They perform if-then checks to ensure transactions are conducted securely. A logistics operator might utilize a smart contract to automate payment upon the items' arrival at the port [24].

2.1.2.THE TYPES OF BLOCKCHAIN NETWORKS

Blockchain technology has proven great advantages for supporting multiple aspects of artificial intelligence applications[17]. Therefore, it is possible that combining blockchain technology with artificial intelligence will lead to new solutions by facilitating the construction of decentralized and collaborative systems at the same time. Many types of blockchain systems are designed to work with artificial intelligence applications[6], [17]. Figure 2 shows the types of blockchain:



Blockchain Types

	Type One Only Cryptocurrency C2C	Type Two Cryptocurrency+ Business B2C	Type Three Only Business B2B
Mode of Peer Participation	Permissionless blockchain Public blockchain	Permissionless blockchain Public or Private blockchain	Permissioned blockchain Private blockchains
Consensus Mechanism	Proof-of-Work (PoW)	Proof-of-Work (PoW)	Pluggable Consensus Algorithm, currently it PBFT
Scalability	High Node-scalability and Low Performance scalability	High Node-scalability and low Performance scalability	Low Node-scalability High Performance scalability
Cryptocurrency	Built-in cryptocurrency called (Bitcoin)	Built-in cryptocurrency (Ether)	No built-in cryptocurrency
Programming Language	C++ with very limited programming possibility and difficult application development very.	Smart Contracts written in Solidity with high possibility for developmet(Dapp)	Chaincode written in Golang with high possibility for developmet

Figure 2: the types of blockchain [25]

2.1.3 Hybrid blockchain network

Hybrid blockchains integrate features from private and public networks. Companies can establish private, permission-based systems in addition to public ones. They regulate access to particular data within the blockchain while making the remaining data accessible to the public. Smart contracts are used to enable public members to verify the completion of private transactions. Hybrid blockchains allow public access to digital currency while maintaining the privacy of bank-owned currency.

1- Consortium blockchains network:

Consortium blockchain networks are governed by a group of organizations[26]. Selected organizations are responsible for upholding the blockchain and deciding on data access permissions. Consortium blockchain networks are favored by industries where multiple organizations share common goals and benefit from collective accountability. The Global Shipping Business Network Consortium is a nonprofit blockchain consortium focused on digitizing the shipping sector and enhancing communication among maritime industry players.

2.1.4 BLOCKCHAIN-AS-A-SERVICE

Blockchain as a Service (BaaS) is a cloud-based managed blockchain service offered by a third party. You may create blockchain applications and digital services with the cloud provider enabling the infrastructure and blockchain development tools without requiring significant infrastructure setup or maintenance [27]. You only need to tailor the current blockchain technology, which increases and simplifies the use of blockchain in various applications[28].

Blockchain-as-a-Service models:

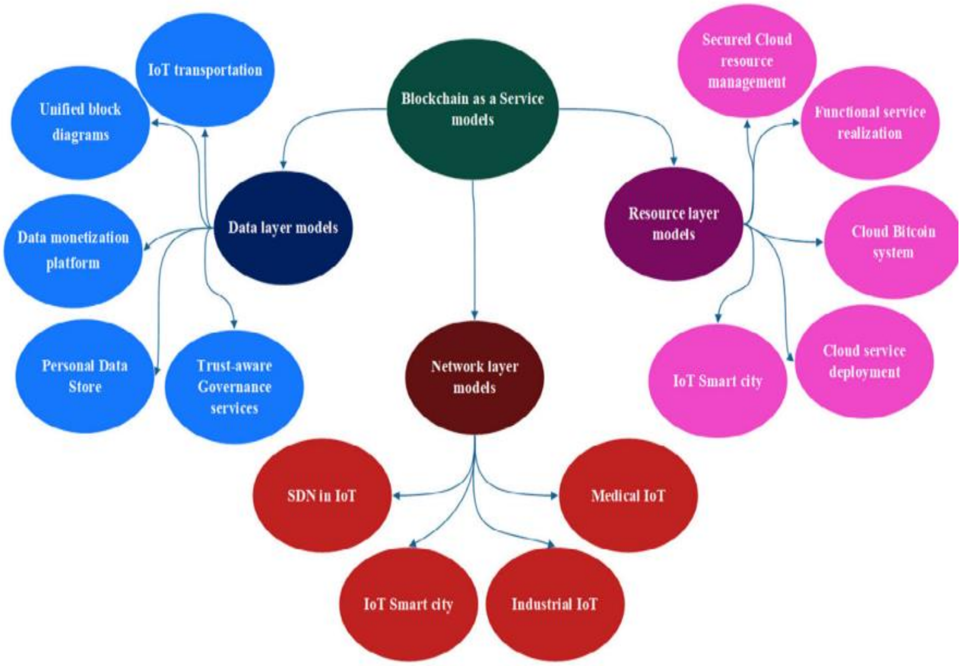


Figure 3: Blockchain-as-a-Service models[28]

2.2 Machine learning concept

Machine learning is a field of artificial intelligence and computer science that employs data and algorithms to simulate human learning processes, enhancing its accuracy over time[29]. Data analysis, pattern recognition, and prediction or decision-making are the fundamental elements of ML which involves the construction of algorithms. The three types of ML are demonstrated below :

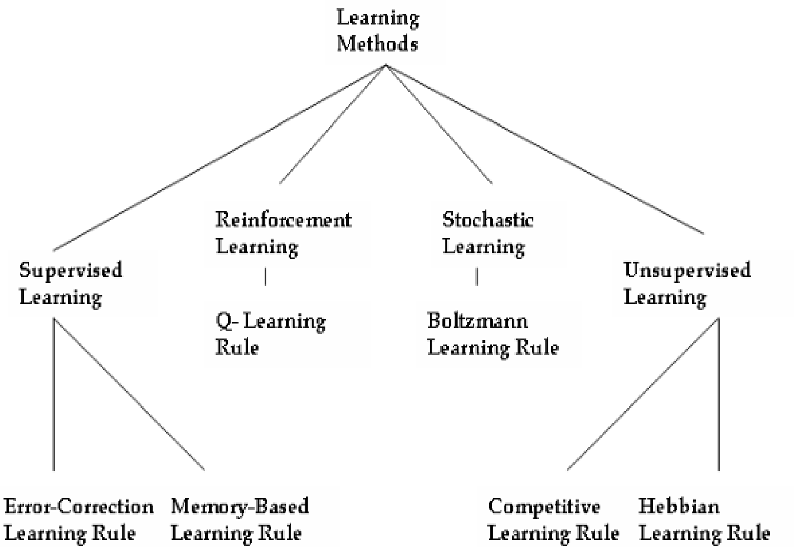


Figure 4: types of ML[30]

2.2.1 Deep learning

Deep Learning is a subset of machine learning that involves neural networks with multiple layers, known as deep neural networks[1]. These networks are inspired by the structure and function of the human brain. Deep Learning architectures are capable of automatically learning hierarchical representations of data, allowing them to capture intricate features and patterns. Key elements of deep learning include:

1- Neural network: A neural network consists of interconnected nodes organized in layers, mimicking the structure of the human brain. Each node or neuron processes information and contributes to the overall computation[31] .

2- Deep neural network: These networks consist of multiple hidden layers between the input and output layers. Deep architectures allow modeling of complex relationships and extracting features from data[32].

3- Training: Deep learning models are trained using large sets of data through a process called backpropagation. During training, the model adjusts its parameters to minimize the difference between the expected and actual outputs.

2.2.2. General Model of Convolution Neural Network

Convolution neural networks (CNNs) consist of numerous hidden layers in addition to a single input and output layer. A specific neuron receives an input vector X and uses function F to produce an output vector Y [33]. This neuron's general equation is provided below, Activation function in convolutional neural networks (CNN).

$$F(X,W)=Y \qquad (1)$$

where W represents the weight vector, which indicates how strongly two adjacent layers' neurons are connected. Then, the resulting weight vector can be employed to perform processes such as image classification. On the other hand, contextual data such as the image's shape provides superior results. CNN is a model that is gaining popularity due to its ability to classify data depending on contextual information. Figure 1 shows the general framework that describes the CNN workflow.

Feature learning
Classification
Output

Figure 5: CNN process steps

Four stages comprise a general CNN model: input data, feature learning, classification, and output. An illustration of CNN elements is shown in Figure 1.

1- **Input:** The initial layer receives the raw input data, typically images in computer vision applications.

2- **Feature learning:** Convolutional and pooling layers work together to extract hierarchical features from the input data.

Convolution layers: The image classification process is done by inserting the image to be classified into the input layer to extract and process the features. The output is the predicted class label computed using the features extracted from the image. The neurons of each layer are connected to several neurons in the next layer. This local connection is known as the receptive field. The receptive field is used to extract the local details from the input image.

A weight vector is formed by the receptive field of a neuron associated with a specific location in the preceding layer. This vector is constant across the plane, which represents the neurons in the subsequent layer. Since all of the neurons in the plane carry the same weight, it is possible to identify similar features in the input data that appear at several places. Figure 6 shows the connection field between layers.

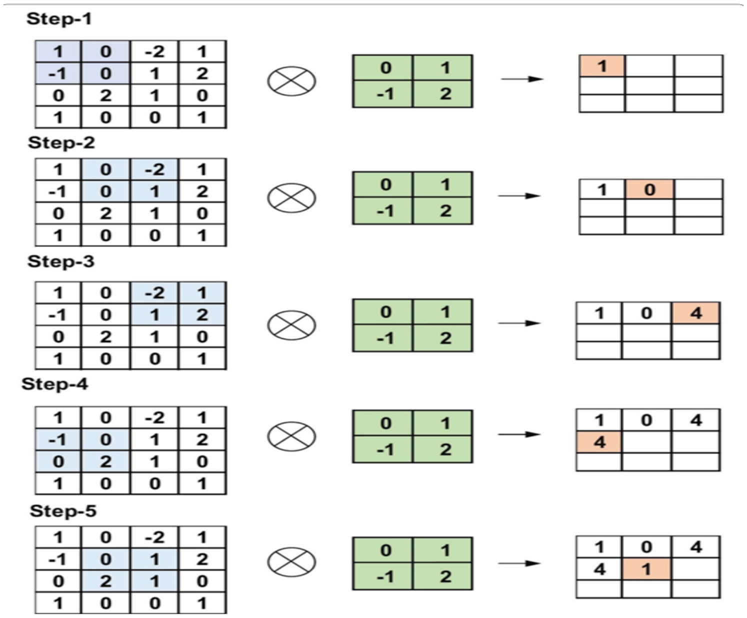


Figure 6: Receptive field of a particular neuron in the next layer[1]

To create the features map, the weight vector (known as a filter or kernel) slides across the input vector. Convolution operation is the process of sliding the filter both vertically and horizontally. Using this technique, N different features are extracted from the input image in a single layer, resulting in N filters and N feature maps.

The local receptive field phenomena cause a large reduction in the number of parameters that can be trained. Following the application of the convolution process, the output for position (i,j) in the following layer is calculated using the formula as shown below, Convolutional Function and Activation Function in Convolutional Neural Networks (CNN) Layers :

$$a_{ij} = \sigma((W * X)_{ij} + b) \qquad (2)$$

where X is the layer's input, W is a filter or kernel that slides over the input, b is the bias, * denotes the convolution operation, and σ represents the network's introduction of non-linearity. [34].

Pooling Layer: when a feature is identified, its precise position loses significance. Therefore, the pooling layer comes after the convolution layer. Using the pooling technique has the main benefit of significantly reducing the number of parameters that may be trained and establishing translation invariance. A window is chosen, and the input items included inside it are run through a pooling function to carry out a pooling process [34], as illustrated in Figure 7.

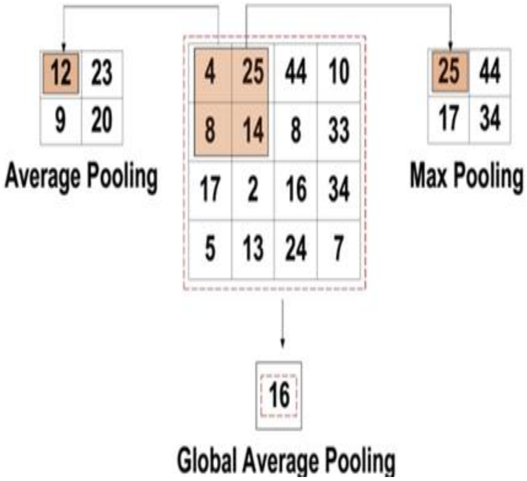


Figure 7: Pooling Layer[1]

3- **Classification:** the first step in classification is **Flatting** in which the high-dimensional feature maps are grouped into a vector. Then, fully connected layers process the flattened data for classification or regression tasks.

4- **Output:** The final layer produces the model's output, providing predictions or scores.

CNNs are widely used in image classification, object detection, segmentation, and various computer vision tasks. Their ability to automatically learn hierarchical representations makes them powerful tools for extracting meaningful features from complex data structures like images.

2.3 Types of datasets

To train models for blockchain and deep learning algorithms, it is necessary to have datasets that are specifically relevant to the desired application. Below is a Figure showing the types of data:

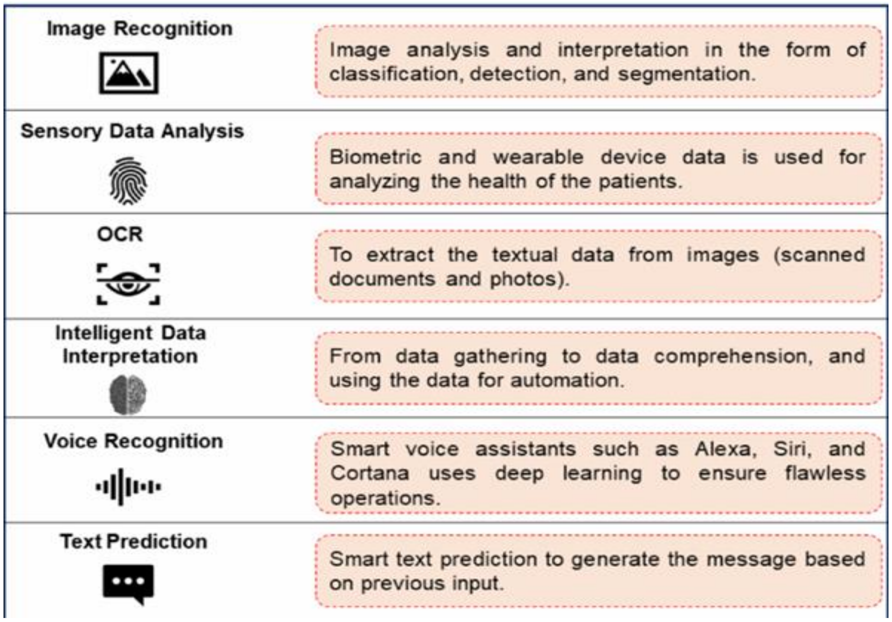


Image Recognition	Image analysis and interpretation in the form of classification, detection, and segmentation.
Sensory Data Analysis	Biometric and wearable device data is used for analyzing the health of the patients.
OCR	To extract the textual data from images (scanned documents and photos).
Intelligent Data Interpretation	From data gathering to data comprehension, and using the data for automation.
Voice Recognition	Smart voice assistants such as Alexa, Siri, and Cortana uses deep learning to ensure flawless operations.
Text Prediction	Smart text prediction to generate the message based on previous input.

Figure 8: types of data[35]

3 Related works

This section presents recent research publications that focus on the integration of blockchain technology with artificial intelligence techniques.

1. **In the paper** [36]**,** a blockchain privacy system (BPS) for a diet recommendation system for patients with special needs has been presented. The system uses machine and deep learning algorithms to analyze an Internet of Medical Things (IoMT) dataset. The long short-term memory (LSTM) technique is found to be more effective than other schemes in terms of prediction accuracy, precision, F1 measures, and recall in a secured blockchain privacy system. The system achieves 97.74% accuracy using the LSTM deep learning model, with a precision of 98%, recall, and F1-measure of 99% each for the allowed class. The proposed BPS system is outstanding, as none of the earlier revised works of literature described a recommender system of this kind.

   Surveillance cameras are crucial in smart cities for crime prevention and security.

   However, authenticity concerns arise. A blockchain-based system was proposed.

2. **in the paper** [37] to ensure the trustworthiness of stored recordings, allowing authorities to validate authenticity. This system discriminates fake videos from original ones and prevents copyright infringement. The distributed ledger records metadata, securing possession and identity for law enforcement and users.

3. **Paper** [38] explored the use of blockchain technology for secure storage and exchange of medical records. This study introduces a website that utilizes blockchain technology for storing and sharing

medical records to reduce the risks of data loss and corruption. The solution utilizes smart contract technology on the Ethereum platform to oversee file generation and sharing, guaranteeing worldwide access for authorized clinicians. The interplanetary file system guarantees strong security and privacy, enhancing the safety and availability of medical records for everyone.

4. **In the paper**[39], the researchers outline an intelligent system for monitoring and ensuring security and attendance by combining these functions with networked surveillance video. It proposes a sliding average method for identifying identities, with experimental results demonstrating a correct identification rate of 98.85% and a false reject rate of 0.51% and 2.52%, respectively. The system facilitates passive, non-intrusive attendance as well as simultaneous attendance from multiple individuals.
5. **The research demonstrates in the study** [40], the utility of a particular video analytics framework based on deep learning for a variety of applications involving process compliance, customer analytics, security, and safety. The study describes the fundamental components of the video analytics system, such as face detection and recognition, object detection, tracking, and human and face sub-attribute analytics. The focus was on utilizing unique models trained with data from deployment scenarios to attain greater accuracy than pre-existing models. This method enhances the system's ability to withstand faults and maintain functionality, increasing its resistance to malicious deviations or failures of individual nodes.
6. **The paper**[41] described the creation of a new optimization technique called Poor and Rich Optimisation using a deep learning model for detecting intrusions in Cyber-Physical Systems (CPS) that utilize blockchain technology. The method employs an Adaptive Harmony Search Algorithm (AHSA) for feature selection and an attention-based bi-directional gated recurrent neural network (ABi-GRNN) model for intrusion detection and classification. The ABi-GRNN technique's detection efficiency is improved by utilizing a hyperparameter optimizer based on poor and rich optimization methods. blockchain technology was used to improve security inside the CPS environment.
7. **Within the article** [42]**,** the authors proposed a Crime Monitoring System (CMS) that uses CCTV cameras to detect crimes in real-time and notify law enforcement. The CMS uses deep-learning methods and image-processing techniques to detect weapons, violence, and faces. Transfer learning models and face recognition algorithms are used for weapon detection and violence detection. The model's performance in real-world scenarios is outstanding, with over 80% accuracy in weapon detection, 95% accuracy in violence detection, and 97% accuracy in face recognition. This system counterbalances human weaknesses in crime detection.
8. The development of a smart building security system with intelligent face detection and recognition has been addressed in the **study**[43]. By utilizing artificial intelligence to improve the system, the goal of the technology was to enhance video monitoring in buildings. According to studies on facial recognition and image capture for cloud storage, the system can broadcast and detect human faces, whether legal or unauthorized. In this study, an investigation of image capture and storage from two different cloud storage types (Dropbox and Cloudinary Dropbox cloud storage) achieved the best performance features, with an image quality of more than 75%.
   The system needs a WiFi connection and a private network with encrypted usernames and passwords for security. The article also addresses the significance of Internet of Things-based smart building solutions . Using the Haar Cascade approach, the system can identify human names recorded in the dataset; for unauthorized users, it displays 'Unknown'.
9. **Khan et al.'s study [44]** objective was to integrate blockchain technology to provide sustainable and resilient smart solutions for intelligent vehicle-distributed video networks, hence eliminating the requirement for third-party intermediaries. Extensive experiments and research provided evidence of the usefulness and practicality of the proposed video blockchain technology. The findings demonstrated that the new framework offers improved security, privacy, and scalability for intelligent vehicle-distributed networks in smart cities, hence facilitating the development of a connected and efficient city.

10. **According to the paper** [44], by employing deep learning approaches for early weapon identification, the study aimed to improve video surveillance systems in banks. The authors provide a framework to minimize false alerts and stop armed robberies in banks and other public places by using real-time object detection systems like YOLO and SSD. To prevent armed robberies, the study shows the significance of security and safety in the modern environment as well as the necessity of prompt action. The importance of high-quality images and the trade-off between model performance and time responsiveness in surveillance applications were also addressed by the authors.
11. **Within the paper** [45] the approach presented was to combine blockchain technology, the Internet of Things (IoT), and deep learning-based image processing to improve management and traceability in agricultural greenhouse operations. The suggested system combines very accurate image processing algorithms with a 98% success rate to automate image capture, measurement, storage, and monitoring of environmental parameters in greenhouses. Using blockchain technology improves traceability across the agricultural supply chain by creating an unchangeable and transparent record of transactions and data points. The paper explores the potential advantages of automating plant head identification and analysis in precision agriculture with deep learning, including better yield prediction, disease detection, and breeding. Using Ganache as the test network, the authors also present a simulated blockchain model appropriate for use in a smart farming setting.
12. **Within the paper** [46] The technique for human fall detection in the document uses a single camera video sequence and is divided into two sections: object detection and fall model application. An adaptive background subtraction method was used in this method to identify moving objects and associate them with their minimum-bounding box. The fall model analyzes, detects, and verifies falls using a collection of extracted features. People and their behaviors are continuously monitored using a two-state finite state machine (FSM).
13. **The authors of the paper**[47] developed a new hyper ledger blockchain-enabled secure medical data management model called HBESDM-DLD. The model involves encryption, optimal key generation, hyper ledger blockchain-based secure data management, and diagnosis. It allows users to control access, hospital authorities to read/write data, and alert emergency contacts. The model uses the SIMON block cipher technique and group teaching optimization algorithm for optimal key generation. Performance validation on a benchmark medical dataset demonstrates its superiority.
14. **Within the paper** [48] a framework using consortium blockchain and deep learning was proposed to identify and prevent such fraud. The model BERT-LE evaluates the reasonability of ICD disease codes for Medicare reimbursement. The solution also ensures data security, immutability, traceability, and auditability.

    The Internet of Things (IoT) is transforming urban architecture and providing public services, but it also poses security risks due to hackers attacking connected devices. To address these issues**, in the study**[49], a Blockchain-Assisted Secure Smart Home Network (BSSHN-GBOHDL) model was developed, which uses BC technology to improve data confidentiality and identify malicious activities. The approach uses data preprocessing, HDL-based classification, and GBO-based hyperparameter tuning. Experimental validation shows a maximum accuracy of 98.29%, outperforming other methods.
15. **The paper** [50] presents a novel video surveillance system that proposes two models using Deep Convolution Neural Network (DCNN) architecture on a large standard database, CASIA-D. The DCNN model is superior in building an accurate gait recognition system on large standard datasets.

    Machine learning and deep learning-based systems can be adapted to monitor suspicious activity, but hybrid or enhanced systems are needed for accuracy and precision. A research study of **the paper** [51] introduced an enhanced convolutional neural network (ECNN)-based system for suspicious activity detection, achieving high accuracy, precision, false-positive rate, and false-negative rate. The authors found that their findings can enhance pre-suspicious activity alert security systems to avoid risky situations.

16. **Within the reference**[52] the study examines the most recent developments in building sensors and environmental monitoring systems. It includes communication technologies, a range of sensor technologies, and the best placement techniques for sensors. Temperature, carbon dioxide, humidity, occupancy, light, and airflow measurement technologies are among the most important and well-known sensor technologies covered in the paper. Other communication technologies and protocols covered include Ethernet, PLCC, Serial Communications, Modbus, BACnet, Zigbee, Bluetooth, BLE, WiFi, EnOcean, 6LoWPAN, Z-Wave, and LoRaWAN. It also discusses the difficulties and potential outcomes of implementing sensing and environmental monitoring technology in buildings, such as data processing, energy harvesting, network security, and the development of IoT and energy harvesting systems for buildings.
17. **The paper**[53] offers a brand-new strategy dubbed BDSDT, which combines deep learning and blockchain technology to guarantee safe data transfer in Internet of Things-enabled healthcare systems. Using two datasets, CICIDS-2017 and ToN-IoT, the proposed BDSDT framework achieved close to 99% accuracy, outperforming state-of-the-art approaches in both non-blockchain and blockchain contexts.
18. **The article in the paper**[54] suggests a plan to guarantee the integrity, decentralization, and security of manufacturing data in smart cities by using blockchain in a distributed fashion at the fog layer. In smart cities, deep learning has been used at the cloud layer to boost output, automate data processing, and improve communication capacity for smart manufacturing and smart industrial applications. Based on the suggested system, open research issues are explored and the proposed scheme has been contrasted to research studies that already exist. The article discusses relevant projects, obstacles, and issues in smart manufacturing in a smart city and offers a case study of auto production with service scenarios. Additionally, it compares the suggested plan with conventional architecture or techniques, talks about the drawbacks of current practices and technological advancements, and suggests a framework for automated, safe smart manufacturing that uses consortium blockchain for privacy and security.
19. **The paper** [55] suggests a deep learning-blockchain integrated ecosystem for evaluating Electronic Health Records (EHR) and enabling patient notifications. It focuses on utilizing the Inter Planetary File System protocol to store EHR on the Hyperledger Fabric using a blockchain-RNN algorithm, and then using deep learning mechanisms—more precisely, Long-short-Term Memory and Gated Recurrent Units—to analyze the data.
20. **In the paper**[56] The DeepCoin framework is a novel system that combines deep learning and blockchain technology for secure and efficient energy exchange in smart grids. It uses a blockchain-based scheme with five phases and a deep learning-based scheme for intrusion detection. The framework addresses security and privacy concerns in smart grids and provides a peer-to-peer energy trading mechanism. It also employs recurrent neural networks for detecting network attacks and fraudulent transactions.
21. **The paper**[57] proposed an approach using deep learning techniques of residual neural networks for proficient anomaly detection in surveillance videos. The study discusses the challenges in PC vision and the use of deep learning methods for identifying threatening actions from video surveillance cameras. Furthermore, this study includes discussions on various aspects of anomaly detection, such as confusion matrix, anomaly score, and image. segmentation, and case studies on road accidents, crime scenes, and explosions. This paper presents a deep learning framework using SlowFast Resnet50 and Softmax function. The framework was applied to the UCF-Crime dataset, achieving 47.8% more accuracy than the state-of-the-art method and good accuracy compared to other approaches.
22. **The paper**[58] discusses the importance of automated object detection and face recognition in surveillance systems, comparing the accuracy and speed of various approaches. The report also outlines the workflow of the proposed video surveillance application, emphasizing the balance

between accuracy and speed. It includes details about object detection, visualizing results, archiving data, and conducting experiments to evaluate trained models. Additionally, it mentions the potential future improvement of using Convolutional 3D (C3D) for video processing**.**

23. **The paper** [59] explores the use of video blockchain technology in smart cities to establish connectivity among vehicles. It uses location-based visualization and multiple cameras to collect video surveillance data, enhancing situational awareness. The decentralized nature of blockchain is used for secure, tamper-proof solutions. Experiments show the proposed video blockchain approach provides enhanced security, privacy, and scalability, paving the way for a connected urban environment.

A lightweight deep learning model for object detection in video summarization was presented **within** [60]. This paper investigates the problem of query-based video summarization construction. Using images and video datasets, the system trains networks using YOLOv3 and Tiny YOLOv3 models. The most relative frames to a given query are selected and assembled as keyframes using a modified K-mean clustering scheme. The system achieved an average object detection accuracy of 93% and 83%, with an efficient summarization rate of 33%.

Table 1: Papers information

Reference number	**Dataset**	**Methodology**	**Metrics**
[36]	Medical Things (IoMT) dataset includes data of 50 patients with various diseases.	Blockchain privacy system (BPS) and machine learning classifiers.	1- Accuracy 2- Precision 3- Recall 4- F1-measure
[37]	Video	Blockchain-based system to ensure the trustworthiness of stored recordings	Accuracy
[38]	records stored and shared through cloud-based central data centers	Using contract technology in Ethereum to manage file creation and sharing, ensuring global accessibility for authorized doctors.	Data Accessibility and Security Safe Storage of Data Cost Safety in Sharing Access to Data
[39]**.**	Video	The MTCNN algorithm is used for face detection. (CNN) is constructed for face recognition and classification, combining the network structure design of AlexNet and Inception.	1- false reject rate (FRR) 2-false accept rate (FAR) 3- correct identification rate (CIR)
[40]	Classroom Dataset Community Center Dataset Traffic Dataset	Deep learning-based video analytics system for security, safety, customer analytics, and process compliance.	accuracy and mAP
[61]	NSL-KDD-2015 dataset	Technique PRO-DLBIDCPS (Poor and Rich Optimization with Deep Learning Model for Blockchain-Enabled Intrusion Detection in CPS) for intrusion detection in the CPS	precision, recall, accuracy, F-score, and

		environment pre-processing, feature selection using an adaptive harmony search algorithm (AHSA), classification using an attention-based bi-directional gated recurrent neural network (ABi-GRNN), and hyperparameter optimization using the PRO algorithm	training/testing time (TST/TGT)
[42]	Images Videos	1-Behavioral Pattern Detection 2-Object Detection 3-Camera Surveillance 4-Deep Learning Models: Deep learning models such as YOLOv5 and MobileNetV2 for surveillance and analysis of video data. 5-Comprehensive Crime Detection	-1Accuracy -2Precision -3Recall -4F1 Score
[43]	Images Videos	the Haar-Cascade method and histogram of oriented gradients (HOG) for face detection and recognition	Accuracy

[44]	Images	YOLO (You Only Look Once) and SSD (Single Shot Multi-Box Detector).	Average Precision (AP):
			Mean Average Precision (mAP):
			Average Recall (AR):
			Precision-Recall (PR) Curve:

[62]	MySQL database Images	the integration of deep learning-based image processing, blockchain technology, and (IoT)	Precision
[63]	Videos	Object detection using an adaptive background subtraction method with a Gaussian Mixture Model in the YCbCr color space to continuously monitor human behavior.	accuracy, specificity, and sensitivity
[64]	Image	1- SIMON block cipher-based encryption 2- GTOA-based optimal key generation: 3- Hyperledger blockchain-based secure data management 4-VAE-based diagnosis	precision, recall, accuracy, F-score, and Kappa
[48]	the blockchain distributed database that stores and manages medical data in a decentralized manner	utilizes a combination of deep learning, specifically the BERT-LE model, and consortium blockchain technology. The BERT-LE model is used for text classification	average precision, recall, and F1-score
[65]	images	Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer With Hybrid Deep	-1Accuracy (accu) -2Precision (perc) -3Recall -4F-score (F)

[50]	use of the CASIA-D dataset for gait recognition Images Videos	The model was trained using a deep convolutional neural network (DCNN) architecture, specifically VGG-19. In the testing phase, the trained model is used to classify the unlabeled images and recognize humans in surveillance systems.	accuracy, precision, recall, and F1-score
[66]	Videos	the use of enhanced convolutional neural networks (ECNN) and surveillance video to detect suspicious activities The system uses a dataset with labeled behavior and employs methods such as human detection by background subtraction, feature extraction by CNN, and activity detection by discriminative deep belief network (DDBN)	accuracy, precision, false positive rate, and false negative rate
[52]	Images Videos	Optimization strategies for sensor placement energy harvesting techniques, data processing and analysis, and considerations for network security	Accuracy
[53]	1- ToN-IoT 2- CICIDS-2017	BDSDT (Blockchain-orchestrated Deep Learning Approach for Secure Data Transmission) utilizes blockchain and deep learning techniques for secure data transmission in IoT-enabled healthcare systems. also mentions the use of the Zero Knowledge Proof (ZKP) mechanism for ensuring data integrity and secure data transmission.	Precision Accuracy Detection Rate False Alarm Rate F1 Score
[54]	DeepBlockScheme utilizes deep learning and blockchain to ensure the integrity, decentralization, and security of manufacturing data	Using of deep learning for data processing and analysis at the cloud layer, while blockchain technology is utilized at the fog layer for securing communication and storing data on an immutable ledger	security and privacy tools
[67]	Electronic Health Records (EHR)	Storing the EHR in the Hyperledger Fabric using the Inter Planetary File System (IPFS) protocol. The stored EHR is then analyzed using deep learning mechanisms, specifically Recurrent Neural Network (RNN) algorithms such as Long-short-Term Memory (LSTM) and Gated Recurrent Units (GRU)	precision, recall, and F1 score
[56]	-CICIDS2017 dataset: -Power System dataset -Bot-IoT dataset:	-System model: -Data acquisition and pre-processing: -Deep neural network classification: -Performance optimization:	-Accuracy: -Detection Rate: -False Alarm Rate:

[57]	Video	Involves five stages in the software part of the system: data collection, pre-processing data, data splitting (train & test), model building, and model evaluation/deployment	confusion matrix, classification accuracy, misclassification rate, recall, precision, F-measure
[58]	-PASCAL VOC: PASCAL VOC 2007 and PASCAL VOC 2012 are -COCO: . -Open Images Dataset (OID): -VGGFace2: -YouTube Faces DB:	Integrating object detection and face recognition methods into commercial video surveillance systems using state-of-the-art algorithms. For object detection, used original implementations of Faster R-CNN and SSD In the application stage, the trained models are applied to a real video surveillance system.	Mean average Precision (mAP)
[59]	Video	blockchain is used for vehicle-based surveillance, integrating cryptographic functions for security.	security, privacy, and scalability
[60]	images and video datasets	YOLOv3 and Tiny YOLOv3 models	The system achieved an average object detection accuracy of 93% and 83%, with an efficient summarization rate of 33%.

4 Results analysis and discussion

Table 2 presents a number of researches and their results in the field of integrating blockchain technology with machine learning algorithms to develop smart video surveillance systems. In addition, this table reviews the results of each algorithm in term of accuracy. In addition, a comparison view and results analysis will be presented. From this table, one can observe that deep learning algorithms such as CNN and LSTM algorithms demonstrate high accuracy values as shown in ref. 51 and Ref. 34, respectively . It can be noted that in most of the studies presented in Table 2, the accuracy measure was used as a basic indicator to test the quality of the used algorithm. In addition, the presented studies showed that using blockchain technology to protect data and adding artificial intelligence algorithms to process cloud data gives effective results. In this paper, we present a set of previous studies on blockchain technology with deep learning that we will benefit from in our research on a security system for monitoring buildings using deep learning models with Blockchain technology.

Table 2: Comparison of different paper results

Reference number	**year**	**Objective**	**Methodology**	**Accuracy %**
[41]	2022	Building Intrusion detection system	Deep Learning Model for Blockchain Enabled Intrusion Detection in Cyber physical system	98.0
[43]	2021	Intrusion detection systems	neural network (ABi-GRNN)	93.5
[36]	2021	blockchain privacy system for a diet recommendation for patients with special needs	-The long short-term memory (LSTM) technique (deep learning) -Blockchain	97.74
[40]	2018	deep learning-based video analytics system for security	CNN for Deep Face Recognition	91.00
[49]	2023	Blockchain-Assisted Secure Smart Home Network to improve data confidentiality and identify malicious activities.	- Gradient-Based Optimizer With Hybrid Deep Learning Model - Blockchain	98.2
[51]	2022	Suspicious actions detection system	CNN	97.0
[53]	2023	A Blockchain-orchestrated Deep learning approach to secure data transmission in IoT-enabled systems	Blockchain and CNN	99.0
[57]	2022	Detecting abnormal activities from videos	deep learning framework using SlowFast Resnet50 and Softmax function	75.0
[58]	2022	object detection and face recognition approaches for practical video surveillance systems	R-CNN with Inception ResNet V2	97
[60]	2022	object detection in video summarization	deep learning model (YOLOv3 and Tiny YOLOv3 models)	93 and 83

5 Conclusion

In this work, we surveyed and analyzed the state-of-the-art regarding the applications and benefits of integrating deep learning with blockchain technology. We have provided an overview of decentralized storage and blockchain technology and discussed how important problems related to artificial intelligence can be improved and addressed. In addition, we provided a comprehensive taxonomic analysis and blockchain applications related to decentralized deep learning processes and blockchain types. A comprehensive examination of blockchain technology for decentralized data management is examined. Through the studies presented in this paper, we conclude that the integration of blockchain technology with machine learning algorithms can provide many advantages to build a safe and robust environment for exchanging information as well as designing a security system for building monitoring. This adds high reliability to systems that rely on the use of cloud systems. It is worth noting that the CNN algorithm provides impressive results, as explained above in Table 2. Therefore, it can be adopted for future research work to use in the fields of security surveillance systems in integration with blockchain technology. . Finally, Most of the research reviewed in previous studies uses the accuracy measure to test the efficiency of the proposed system. Therefore, we suggest using other metrics such as priesion, recall and F1-score to test the proposed new systems, We also suggest using deep learning models and merging them to form a new model to ensure better results. We can suggest using lightweight deep learning algorithms with blockchain technology.

6 References

[1] L. Alzubaidi *et al.*, “Review of deep learning: concepts, CNN architectures, challenges, applications, future directions,” *J. Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00444-8.

[2] A. S. Elameer, “Feature Extraction Techniques on Facial Images: An Overview,” *Int. J. Sci. Res.*, vol. 6, no. 9, pp. 2015–2018, 2017, doi: 10.21275/ART20176682.

[3] S. A. Jebur, K. A. Hussein, H. K. Hoomod, and L. Alzubaidi, “Novel Deep Feature Fusion Framework for Multi-Scenario Violence Detection,” *Computers*, vol. 12, no. 9, p. 175, 2023, doi: 10.3390/computers12090175.

[4] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, “A blockchain-empowered crowdsourcing system for 5G-enabled smart cities,” *Comput. Stand. Interfaces*, vol. 76, no. January, p. 103517, 2021, doi: 10.1016/j.csi.2021.103517.

[5] I. Al Ridhawi, M. Aloqaily, and Y. Jararweh, “An Incentive-based Mechanism for Volunteer Computing Using Blockchain,” *ACM Trans. Internet Technol.*, vol. 21, no. 4, pp. 1–22, 2021, doi: 10.1145/3419104.

[6] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for AI: Review and open research challenges,” *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

[7] Z. Lv, F. Poiesi, Q. Dong, and J. Lloret, “applied sciences Deep Learning for Intelligent Human – Computer Interaction,” *Appl. Sci.*, vol. 12, no. 22, p. 11457, 2022.

[8] G. Li and W. Liu, “Multimedia Data Processing Technology and Application Based on Deep Learning,” *Adv. Multimed.*, vol. 2023, pp. 1–15, 2023, doi: 10.1155/2023/4184425.

[9] S. K. Jarallah and S. A. Mahmood, “Deep-learning models based video classification: Review,” in *AIP Conference Proceedings*, 2023. doi: 10.1063/5.0161553.

[10] S. A. Jebur, K. A. Hussein, H. K. Hoomod, L. Alzubaidi, and J. Santamaría, “Review on Deep Learning Approaches for Anomaly Event Detection in Video Surveillance,” 2023. doi: 10.3390/electronics12010029.

[11] K. Wang, O. P. Popoola, and K. Wang, “Video-Based Abnormal Human Behavior Video-Based Abnormal Human Behavior Recognition — A Review,” vol. 42, no. April, pp. 865–878, 2016.

[12] M. Dipu Kabir *et al.*, “Novel Deep Feature Fusion Framework for Multi-Scenario Violence Detection,” *Comput. 2023, Vol. 12, Page 175*, vol. 12, no. 9, p. 175, Sep. 2023, doi: 10.3390/COMPUTERS12090175.

[13] Y. Afaq and A. Manocha, “Blockchain and Deep Learning Integration for Various Application: A

Review," *J. Comput. Inf. Syst.*, vol. 64, no. 1, pp. 92–105, 2023, doi: 10.1080/08874417.2023.2173330.

[14] J. Shuja, K. Bilal, W. Alasmary, H. Sinky, and E. Alanazi, "Applying machine learning techniques for caching in next-generation edge networks: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 181, pp. 1–40, 2021, doi: 10.1016/j.jnca.2021.103005.

[15] R. W. Ahmad, H. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Blockchain applications and architectures for port operations and logistics management," *Res. Transp. Bus. Manag.*, vol. 41, no. 1, p. 100620, Dec. 2021, doi: 10.1016/j.rtbm.2021.100620.

[16] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design," in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 2018, pp. 1178–1187. doi: 10.1109/BigData.2018.8622598.

[17] A. Kumar Tyagi, A. S. U, and A. Abraham, "Integrating Blockchain Technology and Artificial Intelligence: Synergies, Perspectives, Challenges and Research Directions," *J. Inf. Assur. Secur.*, vol. 15, no. 5, pp. 178–193, 2020.

[18] K. Govindan, P. Jain, R. Kr. Singh, and R. Mishra, "Blockchain technology as a strategic weapon to bring procurement 4.0 truly alive: Literature review and future research agenda," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 181, no. 1, p. 103352, Jan. 2024, doi: 10.1016/J.TRE.2023.103352.

[19] S. Kayikci and T. M. Khoshgoftaar, "Blockchain meets machine learning: a survey," *J. Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-023-00852-y.

[20] M. Z. Shaikh, N. Dixit, D. Manjunatha, A. Chaudhary, and D. Khubalkar, "Applications of Blockchain Technology and Crypto Currencies: Current Practice and Future Trends," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 4, pp. 30–40, 2024.

[21] J. Chen, K. Li, Q. Deng, K. Li, and P. S. Yu, "Distributed Deep Learning Model for Intelligent Video Surveillance Systems with Edge Computing," *IEEE Trans. Ind. Informatics*, 2019, doi: 10.1109/tii.2019.2909473.

[22] A. R. Sathya and B. G. Banik, "A comprehensive study of blockchain services: future of cryptography," 2020. doi: 10.14569/IJACSA.2020.0111037.

[23] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access*, vol. 7, pp. 727–745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[24] S. Wang *et al.*, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *ieeexplore.ieee.orgS Wang, L Ouyang, Y Yuan, X Ni, X Han, FY WangIEEE Trans. Syst. Man, Cybern. Syst. 2019•ieeexplore.ieee.org*, vol. 49, no. 11, 2019, doi: 10.1109/TSMC.2019.2895123.

[25] S. Sabah Sabry, N. Mahdi Kaittan, and I. Majeed Ali, "Droga do technologii blockchain: koncepcja i rodzaje," vol. 7, no. 4, pp. 1821–1832, 2019.

[26] Y. Bai, Q. Hu, S. H. Seo, K. Kang, and J. J. Lee, "Public Participation Consortium Blockchain for Smart City Governance," 2022. doi: 10.1109/JIOT.2021.3091151.

[27] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G. Yu, "Research advances on blockchain-as-a-service: architectures, applications and challenges," *Digit. Commun. Networks*, vol. 8, no. 4, pp. 466–475, 2022, doi: 10.1016/j.dcan.2021.02.001.

[28] D. Li, L. Deng, Z. Cai, and A. Souri, "Blockchain as a service models in the Internet of Things management: Systematic review," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, p. e4139, Apr. 2022, doi: 10.1002/ETT.4139.

[29] "Applications of Artificial Intelligence in Machine Learning: Review and Prospect," *Int. J. Comput. Appl.*, vol. 115, no. 9, 2015.

[30] R. Sathya and A. Abraham, "Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification," *Int. J. Adv. Res. Artif. Intell.*, vol. 2, no. 2, pp. 34–38, 2013, doi: 10.14569/ijarai.2013.020206.

[31] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. E. Mohamed, and H. Arshad, "State-

of-the-art in artificial neural network applications: A survey," 2018. doi: 10.1016/j.heliyon.2018.e00938.

[32] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, 2017, doi: 10.1016/j.neucom.2016.12.038.

[33] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 33, no. 12, 2022, doi: 10.1109/TNNLS.2021.3084827.

[34] S. Indolia, A. K. Goswami, S. P. Mishra, and P. Asopa, "Conceptual Understanding of Convolutional Neural Network- A Deep Learning Approach," *Procedia Comput. Sci.*, vol. 132, pp. 679–688, 2018, doi: 10.1016/j.procs.2018.05.069.

[35] M. Shafay, R. Wasim Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *SpringerM Shafay, RW Ahmad, K Salah, I Yaqoob, R Jayaraman, M OmarCluster Comput. 2023•Springer*, vol. 26, no. 1, pp. 197–221, Feb. 2023, doi: 10.1007/s10586-022-03582-7.

[36] E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi, and O. D. M. Chiadika, "Blockchain-Secured Recommender System for Special Need Patients Using Deep Learning," *Front. Public Heal.*, vol. 9, no. September, pp. 1–12, 2021, doi: 10.3389/fpubh.2021.737269.

[37] P. W. Khan, Y. C. Byun, and N. Park, "A data verification system for cctv surveillance cameras using blockchain technology in smart cities," *Electron.*, vol. 9, no. 3, 2020, doi: 10.3390/electronics9030484.

[38] M. S. Mohammed and A. N. Hashim, "Protect medical records by using blockchain technology," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 32, no. 1, pp. 342–352, 2023, doi: 10.11591/ijeecs.v32.i1.pp342-352.

[39] K. Sun, Q. Zhao, J. Zou, and X. Ma, "Attendance and security system based on building video surveillance," *Adv. Intell. Syst. Comput.*, vol. 890, pp. 153–162, 2019, doi: 10.1007/978-981-13-6733-5_14.

[40] P. Dubal, R. Mahadev, S. Kothawade, K. Dargan, and R. Iyer, "Deployment of Customized Deep Learning based Video Analytics On Surveillance Cameras," 2018, [Online]. Available: http://arxiv.org/abs/1805.10604

[41] R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, pp. 1–14, 2022, doi: 10.1038/s41598-022-17043-z.

[42] M. M. Mukto *et al.*, "Design of a real-time crime monitoring system using deep learning techniques," *Intell. Syst. with Appl.*, vol. 21, no. May 2023, p. 200311, 2024, doi: 10.1016/j.iswa.2023.200311.

[43] M. H. Khairuddin, S. Shahbudin, and M. Kassim, "A smart building security system with intelligent face detection and recognition," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1176, no. 1, p. 012030, 2021, doi: 10.1088/1757-899x/1176/1/012030.

[44] M. Zahrawi and K. Shaalan, "Improving video surveillance systems in banks using deep learning techniques," *Sci. Rep.*, vol. 13, no. 1, pp. 1–16, 2023, doi: 10.1038/s41598-023-35190-9.

[45] T. Frikha, J. Ktari, B. Zalila, O. Ghorbel, and N. Ben Amor, "Integrating blockchain and deep learning for intelligent greenhouse control and traceability," *Alexandria Eng. J.*, vol. 79, no. August, pp. 259–273, 2023, doi: 10.1016/j.aej.2023.08.027.

[46] V. Vishwakarma, C. Mandai, and S. Sural, "Automatic detection of human fall in video," in *Pattern Recognition and Machine Intelligence*, 2007, pp. 616–623. doi: 10.1007/978-3-540-77046-6_76.

[47] N. Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," *Complex Intell. Syst.*, vol. 8, no. 1, pp. 625–640, 2022, doi: 10.1007/s40747-021-00549-w.

[48] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. P. C. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," *Futur. Gener. Comput. Syst.*, vol. 130,

pp. 140–154, 2022, doi: 10.1016/j.future.2021.12.006.

[49] L. Almuqren, K. Mahmood, S. S. Aljameel, A. S. Salama, G. P. Mohammed, and A. A. Alneil, “Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer with Hybrid Deep Learning Model,” *IEEE Access*, vol. 11, no. August, pp. 86999–87008, 2023, doi: 10.1109/ACCESS.2023.3303087.

[50] N. Rajasab and M. Rafi, “A Deep Learning Approach for Biometric Security in Video Surveillance System Using Gait,” *Int. J. Saf. Secur. Eng.*, vol. 12, no. 4, pp. 491–499, 2022, doi: 10.18280/ijsse.120410.

[51] E. Selvi *et al.*, “Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video,” *Electron.*, vol. 11, no. 24, p. 4210, 2022, doi: 10.3390/electronics11244210.

[52] H. Hayat *et al.*, “The state-of-the-art of sensors and environmental monitoring technologies in buildings,” *Sensors (Switzerland)*, vol. 19, no. 17, 2019, doi: 10.3390/s19173648.

[53] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. Najmul Islam, “A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system,” *J. Parallel Distrib. Comput.*, vol. 172, pp. 69–83, 2023, doi: 10.1016/j.jpdc.2022.10.002.

[54] S. K. Singh, A. EL Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, “DeepBlockScheme: A Deep Learning-Based Blockchain Driven Scheme for Secure Smart City,” *Human-centric Comput. Inf. Sci.*, vol. 11, 2021, doi: 10.22967/HCIS.2021.11.012.

[55] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain, and B. Sundaravadivazhagan, “Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System,” *Front. Public Heal.*, vol. 10, pp. 1–10, 2022, doi: 10.3389/fpubh.2022.905265.

[56] M. A. Ferrag and L. Maglaras, “DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids,” *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, 2020, doi: 10.1109/TEM.2019.2922936.

[57] M. Joshi and J. Chaudhari, “Anomaly Detection in Video Surveillance using SlowFast Resnet-50,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 10, pp. 952–956, 2022, doi: 10.14569/IJACSA.2022.01310112.

[58] J. Xu, “A deep learning approach to building an intelligent video surveillance system,” *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5495–5515, 2021, doi: 10.1007/s11042-020-09964-6.

[59] K. Moolikagedara, M. Nguyen, W. Q. Yan, and X. J. Li, “Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities,” *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173621.

[60] S. K. Jarallah and S. A. Mahmood, “Query-Based Video Summarization System Based on Light Weight Deep Learning Model,” *Int. J. Intell. Eng. Syst.*, vol. 15, no. 6, pp. 247–262, 2022, doi: 10.22266/ijies2022.1231.24.

[61] R. F. Mansour, “Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment,” *Sci. Rep.*, vol. 12, no. 1, pp. 1–14, 2022, doi: 10.1038/s41598-022-17043-z.

[62] T. Frikha, J. Ktari, B. Zalila, O. Ghorbel, and N. Ben Amor, “Integrating blockchain and deep learning for intelligent greenhouse control and traceability,” *Alexandria Eng. J.*, vol. 79, no. August, pp. 259–273, 2023, doi: 10.1016/j.aej.2023.08.027.

[63] V. Vishwakarma, C. Mandai, and S. Sural, “Automatic detection of human fall in video,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4815 LNCS, pp. 616–623, 2007, doi: 10.1007/978-3-540-77046-6_76.

[64] N. Sammeta and L. Parthiban, “Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model,” *Complex Intell. Syst.*, vol. 8, no. 1, pp. 625–640, 2022, doi: 10.1007/s40747-021-00549-w.

[65] L. Almuqren, K. Mahmood, S. S. Aljameel, A. S. Salama, G. P. Mohammed, and A. A. Alneil, “Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer with Hybrid

Deep Learning Model," *IEEE Access*, vol. 11, no. August, pp. 86999–87008, 2023, doi: 10.1109/ACCESS.2023.3303087.

[66] E. Selvi *et al.*, "Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video," *Electron.*, vol. 11, no. 24, 2022, doi: 10.3390/electronics11244210.

[67] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain, and B. Sundaravadivazhagan, "Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System," *Front. Public Heal.*, vol. 10, no. May, pp. 1–10, 2022, doi: 10.3389/fpubh.2022.905265.