SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I4P115

Volume 10 Issue 4, 152-163, April 2023

Original Article

Cybersecurity in Blockchain by Secure Identity Management using Long Short Term Memory (LSTM)

D. Nancy Kirupanithi[1], A. Antonidoss[2], G. Subathra[3], R. Surendiran[4]

[1,2,3]*Computer Science and Engineering & Hindustan Institute of Technology and Science, Padur, Chennai,Tamil Nadu, India.*
[4]*School of Information Science, Annai College of Arts and Science, Kumbakonam, India.*

[1]*Corresponding Author : nancy28988@gmail.com*

Received: 23 February 2023 Revised: 26 March 2023 Accepted: 16 April 2023 Published: 30 April 2023

Abstract - *One of the major technologies in delivering infrastructure and data service requirements at low cost and with minimal effort is Cloud Computing (CC), which has been implemented in several aspects of the IT industry. Since the rapid growth of CC has been observed, there is still an information security concern that intruders completely attack. With the potential of being practised in various utilizations, blockchain can be implemented in several cloud service providers. Blockchain platform has basically performed a large computation quantity which doesn't accomplish the practical purpose of building Proof of Work (PoW) with context awareness accord from decentralized participants. Long Short-Term Memory (LSTM)has been designed particularly for overcoming the long-term dependency issues faced by Recurrent Neural Networks (RNN). This paper focuses on a novel consensus mechanism by LSTM which consists of feedback connections in making a difference with several conventional feed-forward Neural Networks. The research directed computation spent to consensus towards RNN optimization for better cyber security in blockchain implemented in the cloud platform. However, the enormous amount of data involved in the blockchain has been trained through the LSTM model that supports serving learning proof through cell states which handle the network of current long-term memory. Therefore, Contextual Identity Management (CAIM) mechanism is adopted through the LSTM model in blockchain for various Cloud Service Provider (CSP) in unifying the contextual details with the process of identity management that generate the probable robust solution. This assists in creating better decisions with respect to policy, authentication, routing and authorization for recent interacted data. Moreover, the proposed LSTM model in blockchain has been compared with the existing cyber-secured model of blockchain to determine the efficiency of the cyber-secured model of blockchain in the cloud platform.*

Keywords - *Blockchain, Contextual Identity Management (CAIM), Long Short Term Memory (LSTM), Cloud platform, Cloud Service Provider (CSP).*

1. Introduction

An individual has created a digital identity in cyberspace, which perform as an online identity. A digital identity acknowledges the identity owner using certain digital identifiers such as domain name, E-mail address or some URL similar to a passport which assists in identifying the owner for a particular task. The system required can identify expected users and verify the names, addresses, and personalities because the technologies have been moving toward the usage of digital [1,2,5]. Nowadays, the significant component of the internet is the digital identity for accomplishing services from electronic Service Providers (SPs). In this digital world, the user's identity can be represented as digital identity and carry out its required data which permits the identity owner to access several resources over the internet provided by SPs [6]. Operating and securing the user's identity and its associated data and transaction data are the crucial assignment that must be considered. In order to access the necessary services for the authorized users through credentials of digital identity with ease as well as accomplishing tasks with a simple procedure using an organizational process named IDMS. At present, service applications like business services, government services and personalized services are maintained and transforming the personal data of individuals is made significant. Since digital identity on the web has been stored and maintained in certain central repositories that can be handled by third-party management who may tamper and delete user's data without any knowledge of the user's authorization, this may lead to cause security theft, identity theft, etc. Hence, the solution required for this process is a robust Identity Management System (IDMS). Thus, one of the major worldwide problems is digital identity, which must be focused on. Moreover, the benefits of IDMS are by providing better security services, namely privacy, trust management and confidential process from recent available threats and cyber-attacks.

The internet consists of blockchain distribution that covers data blocks in multiple nodes and executes and transmits data with respect to multiple blocks linked together [7]. Each block consists of the previous block hash, which is named a blockchain because of the cryptographic link of all blocks to each block by hash. Hence, if all blocks tried to tamper with any of the blocks, the block hash may not match, and the chain pf the block is meant to be invalid for an immutable ledger feature. The features of blockchain aid in resolving the most significant centralized IDMs problems through data decentralization, individual control and data immutability. These features have provided the users complete control of their data for improving security through the limitation of third-party control, a major disadvantage in centralized IDMS. When none of the entities has acquired data, transparency and security features may avoid the central authority problems. An additional feature is about blocks on a blockchain which can't be modified, and its essential features over security factors play a major role in minimizing attacks [8]. There are several interesting aspects of blockchain integration with IDMS that could solve problems and enhance system performance and user privacy. The most crucial qualities that promote development include decentralization, immutability and transparency. However, there are currently issues that require to be resolved, namely the blockchain system's scalability.

Blockchain Network (BCN) is a decentralized distributed system in which users have the capability to maintain a reliable database or ledger despite collection in which participants have a lack of confidence in one another. BCN is being utilized in cutting-edge financial services like cryptocurrency and smart contracts, both pioneered by the Bitcoin system. It has also been planned to play a significant part in applications that call for long-term, impenetrable data storageThe significant disadvantage of BCN is because Proof-of-Work (PoW) technique that creates consensus among distrustful nodes, which produces better computation as well as energy. Several energy has been consumed on estimating the present hash function that may not generate an exact task which is complex in computing. The energy consumption and computation have been directly spent through blockchain consensus for the possible function of training ML models. The consensus mechanism in the BCN has specified the participants in determining the valid increment for the data ledger or block. However, the valid blocks have been accumulated in the ledger. Hence, the consensus mechanism is the main for the ledger integrity and consistency. In order to resolve the puzzle of asymmetric for the user challenge is PoW, which is familiar and can solve complex data but simple in verification. One of the present instances is considered as x whose hash hx initiates with a particular zero number [10]. Once the present instance is identified, the other individuals can be justified with simple verification when the solution is accurate. After, the problem solver is made to be admitted for appending the recent block to the blockchain. Finally, the block on the chain consists of a hash of the earlier block. Tamper with an old block need regeneration of any subsequent block that is extremely high cost.

In several applications, the context has produced a better intrinsic value to raw data than the required data. Context awareness has figured out neither the data nor related metadata that produce certain supplementary data about an environment circumstances of user, object or devices. Thus, the contest-awareness may generally produce a high-reliability level and beneficial surrounding of the source as well as the data application. Context Awareness is the system which has the capacity to collect data about its environment as well as accommodate behaviour correspondingly. The authentication of context-aware systems has become progressively interesting when mobile devices are in extensive computing environments. It can be implemented in several methods as well as ensuring secured authentication through user behaviour analysis for the devices. A subsequent security layer has been accumulated with blockchain through an authentication system of context awareness by implementing in conjunction with password-based authentication methods. This paper has proposed an authentication system by context awareness that is simple in implementation as well as profitable [11].

A robust Intrusion Detection System (IDS) is necessary to address the underlying problem since typical techniques use a signature-based method to detect distinct configurations. The Deep Extreme Learning Machine (DELM) [12] is an advanced technique that can be employed to analyse data flow to detect intrusions and attack patterns. As a result, it's essential to manage intelligent blockchain-based systems by developing effective and adaptable algorithms to handle this massive volume of data. With no human assistance, machines are included to train, reason and behave using ML, which is regarded as a framework for Artificial Intelligence (AI). The fundamental objective of ML is to develop an efficient algorithm that can use input information to make predictions and alter outcomes through data analysis and statistical analysis. Hence, the DELM technique has assisted in creating secured intelligent home using Internet of Things (IoT) enabled sensor that influences performance. The main contributions of this study are to provide a comprehensive review of cutting-edge technologies relevant to blockchain-based smart homes equipped with the DELM. This presents a new perspective on various applications, namely smart home data sharing, supported by the current stages of technological development. The deployment of DELM architecture in blockchain-based smart homes has been suggested. A blockchain network might handle the DELM framework's datasets, eliminating information flaws such as repetition, loss of data value, inaccuracies, and disruption. Blockchains are data-dependent, so the data-related issues in the DELM framework will therefore be disregarded. Instead of focusing on the complete collection of datasets, the DELM framework

can be used to focus on different chain pieces. This will offer a distinctive foundation for numerous applications, including fraud detection and theft prediction.

2. Literature Review

Various context-aware authentication systems presented in this literature have illustrated the proposal for verifying the authenticity of an authentication request from users by dealing with contextual data using the characterization of the user's environment and behaviour. This literature further discusses the various IDM-based authentication and authorization methodology.

Two major focused literature surveys on IDMS and blockchain in which the earlier studies do not involve are [7, 15]

- Action on IDM using blockchain technology
- Consensus mechanism recognition is considered for evaluation until
- Researchers between the period 2009 and 2016 are evaluated
- This study involves research projects experienced in the technology field of IDM and blockchain.

The requirement for an analytical review and consolidation of the collection of literature in the area of IDM employing Blockchain technology has emerged as a result of the experts' interest in blockchain. However, the mapping with systematic have consumed more time but generated understandable and complete data on the current research. Hence, this research discover that a major IDM framework over the blockchain is involved until it has mentioned the gaps and suggested events for further researchers.

The premise of dynamic authentication is the authentication of users in accordance with accessing data patterns, features extraction from the network, application usage and all subsequent data generated dynamically in real time. The involvement of ML is essential in mining certain data and extracting needed features in accepting or rejecting the users in the system. Moreover, the biometric extraction features obtained from users and behaviour pattern with dynamic analysis has contributed to continued authentication, which has improved cybersecurity security and confirmation of identity over the current basis [17]. A similar authentication scheme is beneficial for users due to the recognization of required daily business gets accomplished has been identified. Since it is not feasible for people to track users continually, ML is the only way to carry out continuous authentication. This assists in solving a challenging issue involving a vast amount of data and several factors to manage dynamic authentication in telehealth. The ideal method is still ML, but choosing the right model for the data at hand is important. To select the ideal model for the current situation, the workflow of data analysis and ML is necessary. Data points of keystroke dynamics have provided distinct features which assist in employing most ML models, including SVM, NB, RF, KNN, and conventional ANN.

Nevertheless, it is preferable to adopt models which can manage sequential data or time series for the analysis of ECG signals, namely Long Short-Term Memory (LSTM), Convolutional Neural Network (CNN) and Hidden Markov Model (HMM). The optimum technique may be employing CNN in authentication systems that use stationary data, such as face recognition. In the case of the traditional method, the basic pattern is extracting certain features from images and progressing with other ML methods. Fard et al. have progressed an autoencoder for influencing the optimum feature space in discriminating every individual in the system and also with respect to its local liner reconstruction error [20]. Thus, the proposed method is the less expensive and better option in using for the authentication system of telehealth, which requires authenticating the users in real time.

A deep CNN classifier is utilised by Zeroual et al. for authenticating users with respect to their face images [21]. This model maintains complex computation by assigning training processes to the cloud due to large data volumes. Abuhamad et al. has explained the LSTM classifier in three various LSTM architectures, bidirectional LSTM as well as multifactor LSTM to authenticate users [22]. Collecting datasets from individuals by measuring magnetometers, gyroscope sensors and accelerometers from mobiles with the frequency of high authentication. In the final classification layer, both represented supervised models have utilized compressed networks. In order to identify human behaviour in mobile and wearable devices, Xia et al. have merged LSTM and CNN layers [23]. The raw data of the gyroscope and accelerometer are involved with LSTM traced by the layer of CNN in generating a robust classifier.

M.A. Bouras et al. have discussed the recent IDM technique in accordance with private blockchain that focused on providing a significant and easy protocol that accommodates all the Internet of Things (IoT) requirements [24]. In the case of smart home model generation, researchers have implemented hyper-ledger fabric and executed the chain codes in the Golang language. IDMS's major functionality has segregated into three phases in order to maintain concurrent execution are

1. Identity revocation
2. Identity verification
3. Identity registration

These three phases have used smart contracts in interacting with blockchain technology. The researcher illustrates the recent model that improves IoT entities' communications using the service of consortium membership and IDM protocol. In order to accomplish high security and

improved scalability, researchers have decided to employ a private blockchain in this model. In the case of behaviour, it is more comfortable with centralization than decentralization which inflation SPOF risk and central authority issues. L.Stockburger et al. have advanced the decentralized IDMS prototype by hyper-ledger finding blockchain as a Proof of Concept (PoC) over the public transportation sector with respect to the principle of self-sovereign identity [26]. This method has minimized the requirement of multi-travel cards for people who generally travel continuously and utilizes various transportation modes in multi-jurisdictions. By establishing a direct identification layer based on the decentralization principles and employing a blockchain-based IDMS in providing users with a Single European Transport, the system seeks to contribute to users' complete identity management. The proposed system allows for the creation of several decentralized identifiers for every individual, as well as the creation of a key pair for each user in facilitating secure data sharing.

X. Xiang, M. Wang, and W. Fan have introduced an IDMS authentication scheme based on permissioned blockchain, which is involved in resolving key management as well as authentication problems over e-health management by a mechanism of key distribution in personal biometrics [28]. The founder, the user, the registration hub, the medical server, and the smart contract that performs access control functions are the four key constituents of the proposed system. The two main conceptual issues are the discrete logarithm problem and the computational Diffie-Hellman problem. The suggested method accomplishes anonymity by masking the user's identity and includes an equation of mutual authentication. To use the Scyther tool, an automatic security protocol verification tool, the designer evaluated the suggested system and ensured that it met the security needs.

S. Wang, R. Pei, and Y. Zhang have introduced Ethereum-based IDM, the improvised version of Consolidated IDM (CIDM) that assists in resolving dependent issues from third-party that are obtained in conventional IDMS [29]. This proposed method has introduced smart contracts to increase data transmission privacy and even improve model flexibility. Gutierrez-

Aguero et al. has introduced a technique which permits users to sign transactions by various Ethereum identities to improve user untraceability by permitting the authorization for the user to delete data as well as acknowledging in discard their identity once completed. The suggested approach implements identity using web3js, and data erasure can be requested by the user or triggered by the end of a service. Gruner, A., Muhle, A. and Meinel, C. have suggested that attribute trust may be improved by adopting an Attribute Trust-enhancing Identity Broker (ATIB) architecture in improving the system attributes aggregation for the subsequent SSI principles. The protocol manager is the key element in the suggested architecture and is capable of supporting the development of numerous identities and access protocols to the system. This may assist the service provider's role to be strengthened as part of the PoC proposal.

3. Research Methodology

The proposed blockchain network has a decentralized Peer-to-Peer (P2P) process consisting of two different entity types, namely data nodes and consensus nodes. Between nodes, communication has been secured through asymmetric encryption of public and private by CAIM. It assists in access in terms of blocks broadcast to the entire network. Let's consider the data node as Cloud Service Provider (CSP) or customer who has used the service application through the Deep Learning technique. LSTM plays a major role in cyber security with CAIM through blockchain. The consensus nodes are considered to be the CSP of the computation power in an application service system. The LSTM is made to train the model that meets the requirements mentioned in the data node. CAIM plays a major role in identifying the best consensus node that received the rewards the data node mentioned and associating multiple identities with the same user. Additionally, the blockchain has functioned as decentralized data, which is awarded from data nodes that stored get identified by CAIM.

Collecting distinct customized resources like networks, servers, services, storage and applications are said to be CC which influences cloud customers for beneficial as well as on-demand access in CSP. CC is used from individual frequencies that referred can be managed by these identities and regulate the access through cloud clients. However, the main issue is about implementing reliable management for identity and access to the system in the cloud, has required for improving venture security. Hence, this research has presented an intelligent and trustworthy CAIM system based on LSTM. The entities involved are data nodes which commission the requesters' tasks to the users (CSP). Request sent through a data node that has the desired identity specification to access the files in the log with better accuracy. The focus of this research is to develop a system that can achieve context-aware identification methods to authenticate real users and access data on the cloud server.

3.1. Working on the CAIM Server

Certain personal details or profiles of devices have been involved in contextual data utilized over the process of recent authentication as well as authorization. Nevertheless, it has been predicted that an entire contextual data amount has been produced through cloud servers and connected devices. The cloud environment states that several contextual factors may be acquired, connected to a particular authentication or authorization request, and used collaboratively to build a more reliable and secure solution. The successful authentication of a user or device and the authorization of a privilege set requires the confluence of several factors.

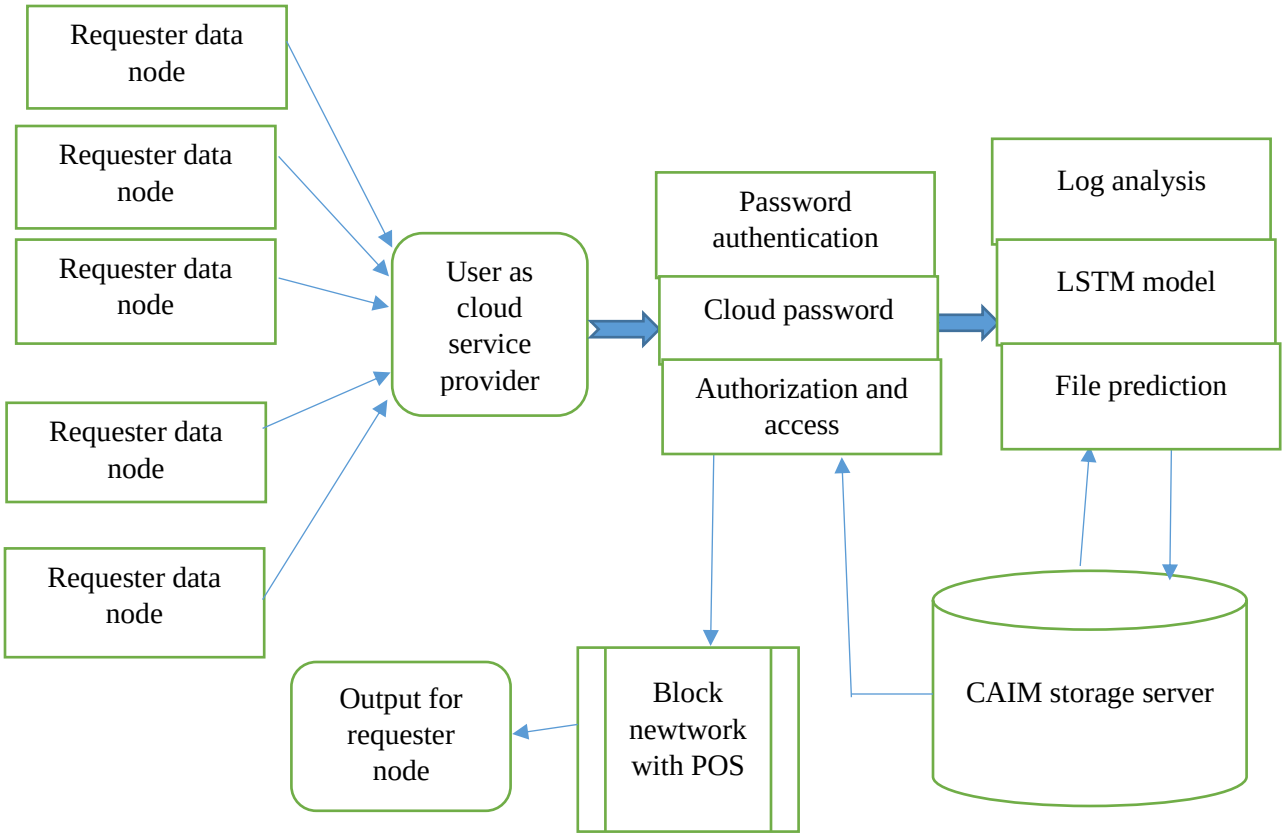

Fig. 1 Cybersecurity architecture for blockchain with LSTM model

The essential factor for IDM is maintaining more identities by user consisting of various identifiers, characteristics, attributes, etc., in which the single user can maintain several identities based on applications and customized design usage. Similarly, the user can have multi-intrinsic identities which support various IP addresses. The CAIM method is generally dynamic due to the accomplishment of several identities within a single user. This facilitates the IDMS in applying awareness about prior or present user behaviour for better decisions with respect to policy, routing, authentication and authorization for the current communication. The complex privacy business has been studied and resolved using this leading capacity.

The basic principle involved in this proposed CAIM-based blockchain with LSTM architecture consists of the context-aware domain that generates and delivers contextual data. CAIM is a suitable pattern which involves contextual data in the user domain, which includes IDM infrastructure. IDM may exist in a similar user domain as a context server that operates inter-domain arrangements. When it is potential to integrate the IDM environment and context server, the pattern is created based on transaction series which interchange the contextual data through request or response among the context user and context CSP environments. In the CAIM-based blockchain with LSTM architecture, the key feature mentioned is the context server because it executes a major role in the domain of the context user. The transaction process in the context server progress with the request or response flow model due to the request received to a particular identifier, acquiring contextual data from the suitable contextual resources and delivering the data in a requesting authentication or authorization engine in the multifactor authentication with LSTM model for context CSP domain.

3.2. Context-Aware Identification Management (CAIM) Framework

The context server emphasises a major role in the transactional view of contextual server storage based on the basic infrastructure of IDM. This has performed a similar user domain or identical with a combined service set and the application of a third party. However, the IDM-based transaction for user service requests and the service arrangement is better in this proposed CAIM-based blockchain architecture. The huge transaction flow of IDMS with the LSTM model can be executed through this CAIM ecosystem. There is no ancillary context needed for the specific identity in the authentication. The context has executed permission for an authenticated identity that incorporates time, location and environment.

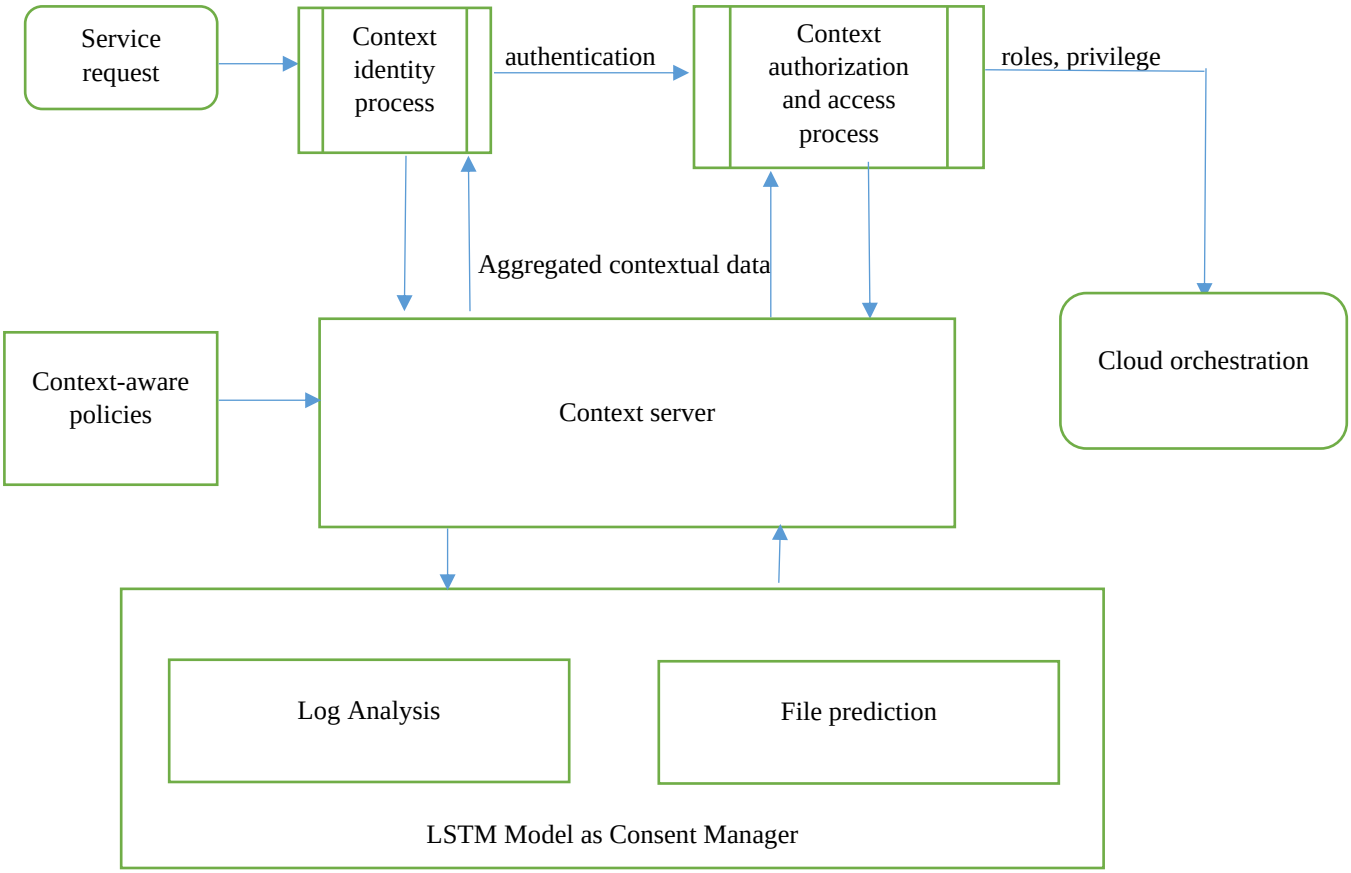

Fig. 2 Framework of Context Identification Management (CAIM)

Furthermore, this might decide or alter the network handles a request made by that identity in regard to the current situation. According to an instance, when a first responder is present at the location, they may be the only individual authorized to upload the footage or update a database about the situation. They might also result in the highest QoS, low latency or resilient routing, or extra security if they are present. Only when the user authorized by contextual components, namely network visibility, location, proximity to other users, etc., have become significant. The necessary subset of all potentially available contextual information may be determined in relation to what the user is attempting to accomplish at the time.

3.3. Context Identity Process

Multifactor Authentication (MFA) is the current approach which has faced a major challenge is about balancing among users' reputation as well as security robustness. Each additional MFA level has increased subsequent complex layer from the user point of view with respect to data in which the user is familiar with either password or certain aspects such as wireless keycards, secure tokens and smart cards. Indeed, passive authentication techniques, which rely on things like user keystroke actions or other biometric features, have emerged due to the convergence of stronger passwords and a lack of user demand for more sophisticated authentication patterns. Context-aware is an effective arrangement which enhances the current and future infrastructure of IDMS.

The contest has been collected from the equipped and supplied to the identity manager that is created through contextual data as well as respective risk factors. When the risk score surpasses a particular threshold, the user has urged to provide supplementary MFA-level data. Moreover, when the contextual data get validated from the user whose action is highly enhanced in traditional MFA methods.

3.4. Context Authorization and Access Process

As a result of authenticated users frequently being assigned particular capabilities and permissions depending on saved profiles and roles, access control and authorization systems have developed utilizing nearby static data. In rare circumstances, privileged access to particular resources may be granted or denied merely based on the user's domain or device making the request. Enhanced authorization of context-based has involved a recent dynamic capability domain in which privileges and permissions are modified through a contextual environment in requesting entity variation at this session. According to an instance, authorization services have been created in accordance with the user's location, the

concurrence of users to other users or CSP in the provided environment or physical factors enclosed by the user. All functions in the context-aware are performed based on the authorization manager with no direct user interferences. Hence, this proposed CAIM with an authorized user can accomplish high experiences and identity domain get enhanced by a better robust solution.

3.5. LSTM Model as Consent Manager

The consent manager is liable to inform the context storage server through the LSTM model that consists of user source as log analysis and file prediction with aggregated data regarding consent on an application basis. User consent is required for authorisation, whereas the contextual data type is utilized by the application in which the location is shared with the financial institution but is not applicable for social media applications. In several cases, the user consent policy has been stored in the consent repository. User consent is essential for acknowledging contextual data for interchanging data in the context server and delivering it to the consumer domain.

Users who choose to endure anonymous get a right to privacy, and all identification systems' awareness of and level of assistance for anonymous activities is an important factor. For key aspects, it is appropriate to assume an identity that can be linked to a specific person. Moreover, when anonymity is not practicable, the end user must also be notified of this constraint. As a result, the user who demands anonymity should have their requests fulfilled but must also be prevented from using services which demand verified identities.LSTM as a context manager, assists in locating an application, and federated services have requested the contextual data related to a particular identifier. The responded data has been utilized in terms of identity and performing access control, which endures with OTT or password as the third-party domain. LSTM model as consent manager has provided the policy of context-aware may accomplish rules and privacy policies of consent with respect to user influences and federation needs.

This working architecture procedure implies that the LSTM as a context manager and CAIM with blockchain as an IDM infrastructure has been located in the same domain and served as a model in the cloud platform of the data flows through this proposed CAIM-based blockchain with LSTM model.

Step 1: Resource for the user is requested through the requester data node and maintains an identity to the resource provider (CSP).
Step 2: MFA produce an identity engine that exists in the same ownership domain as the context manager, or this may be a federated third-party password or OTT domain.
Step 3: MFA engine determines with respect to context-aware policy in which the contextual data need to authenticate the CSP user. It requests contextual data from the LSTM model as a context manager.
Step 4: LSTM model associates the IDM with certain log analysis as contextual data sources and request this data from the contextual environment as file prediction for the requested user.
Step 5: Log analysis is returned to the context server, which is then aggregated, formatted and returned to the MFA engine, reliable with consent and privacy policies.
Step 6: MFA engine has determined, in accordance with policy, when the requester is authenticated over the domain and passed the authenticated user for the file prediction in context manager or denies access.
Step 7: The file prediction in the context manager may optionally request subsequent contextual data from the context server to access definite privileges, roles or delegations.
Step 8: The LSTM model as context manager performs better performance to all requests from the MFA engine.
Step 9: BCN with PoW as the consensus node generates better learning for improving secured nodes and generating better transmission of nodes.

4. Result and Discussion

In this research, the UCI ML repository with crop mapping uses optical-radar and multivariate time series datasets. This dataset consists of 175 attributes and 25,862 observations, and the data gets split into 80% of the training dataset and 20% of the validation dataset.

The sample consists of 5172 observations in which the training dataset and testing dataset are calculated based on the prediction of CAIMbased blockchain with the LSTM model and evaluated through accuracy and loss parameters for 50 epochs with an interval of 10 epochs shown in Figure 3 and Figure 4.

Figure 3 illustrates the accuracy curve for training and validation in which the training accuracy is 0.9831, and the validation accuracy is 0.9580. The model accuracy has improved as the epochs increase, whereas the fluctuation of accuracy occurs till epoch 30 and a very slight deviation from 30 to 50.

Figure 4 illustrates the loss curve for both training and validation in which the training loss is very low with a value of 0.008 and validation accuracy is 0.241. The model loss has reduced as the epochs increase, whereas the loss fluctuation occurs till epoch 40 and a very slight deviation from 40 to 50. The proposed CAIM-based blockchain with the LSTM model is evaluated through a confusion matrix and compared with CAIM with ARIMA, CAIM with CNN, and LSTM, have shown in Table 1.

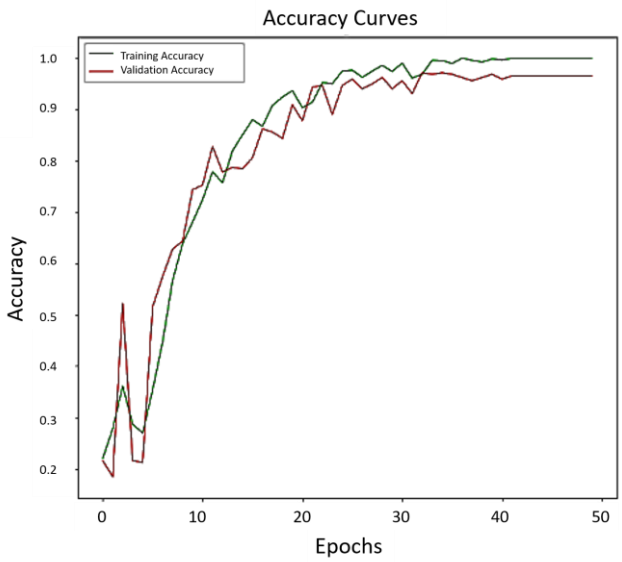

Fig. 3 Accuracy curve for CAIM-based blockchain with LSTM

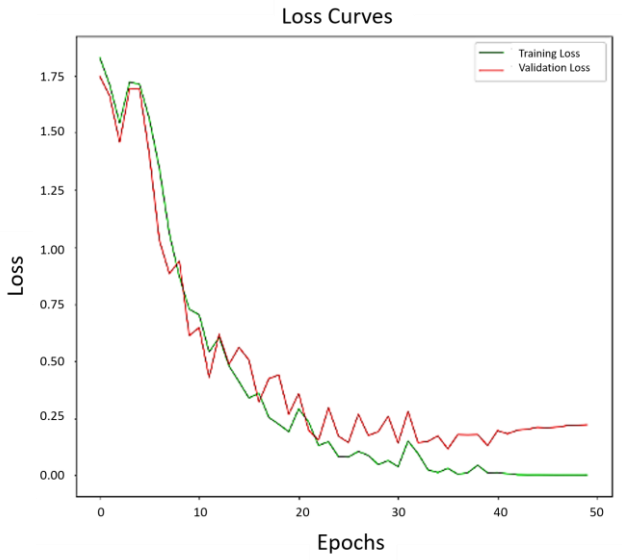

Fig. 4 Loss curve for CAIM-based blockchain with LSTM

Figure 5 illustrates the CAIM based blockchain with LSTM, in which the exact finding of intruder is 104 and the TP value is 2688, representing the exact finding of the non-intruder user. This can be identified through metrics like Accuracy (ACC), false positive rate (FPR), true positive rate (TPR), and F-Measure and detection rate (DR). The CAIM-based blockchain with LSTM should exhibit better TPR, F-Measure, DR, and ACC but with lower FPR.

ACC is the distribution of overall instances correctly classified in terms of TP and TN to the overall sample size of the dataset is expressed in equation 1.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

DR defines the exact classification of sample data and is said to be precise. The ratio of TP to all the instances is provided as an intrusion and is expressed in Equation 2.

$$DR = \frac{TP}{TP+FP} \quad (2)$$

TPR defines the exact classification to a given class division by total instances that involves TP and FN of the class, is said to be recalled and is expressed in equation 3.

$$TPR = \frac{TP}{TP+FN} \quad (3)$$

FPR is defined as the False Alarm Rate that provides the total instance of usual data considered as FP to the usual total data set instances and is expressed in equation 4.

$$FPR = \frac{FP}{TN+FP} \quad (4)$$

F1-Scorediscusses the DR and TPR composed to identify the evaluation measure. The value of the F1-Score is expressed in Equation 5.

$$F1 - Score = 2 * \frac{DR*TPR}{DR+TPR} \quad (5)$$

Figure 6 illustrates the accuracy performance of several blockchains with the ML model. The proposed CAIM-based blockchain with LSTM has produced a better-secured model through its obtained result of 95.80% compared to other models like CAIM with CNN, CAIM with ARIMA and LSTM model.

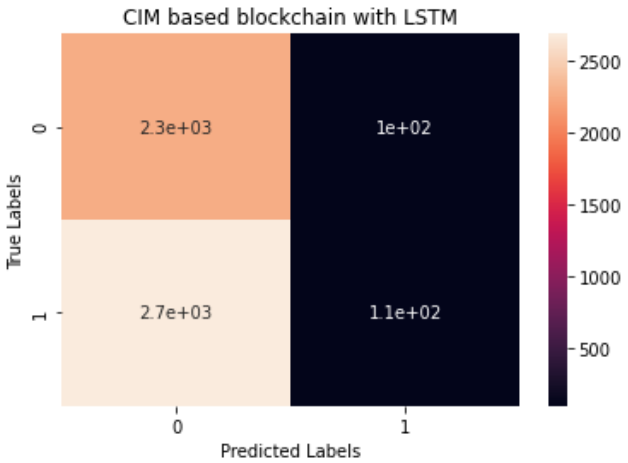

Fig. 5 Confusion matrix for CAIM-based blockchain with LSTM

Table 1. Confusion matrix values for various model

Sl.No	Model Name	Confusion Matrix Values			
		True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)
1	CAIM-based blockchain with LSTM	2688	2267	104	113
2	CAIM-based blockchain with CNN	2635	2266	141	130
3	CAIM-based blockchain with ARIMA	2613	2274	136	149
4	LSTM	2574	2176	214	208

Table 2. Confusion matrix metrics for various model

Model Name	Accuracy (%)	Detection Rate (%)	Recall (%)	FRP (%)	F1-Score
CAIM-based blockchain with LSTM	95.80	96.28	95.97	3.72	96.12
CAIM-based blockchain with CNN	94.76	94.92	95.30	5.07	95.11
CAIM-based blockchain with ARIMA	94.49	95.05	94.61	4.94	94.83
LSTM	91.84	92.32	92.52	7.68	92.42

Figure 7 illustrates the DR performance for several blockchains with ML models. The proposed CAIM-based blockchain with LSTM has produced high detection of intruders, which can be accomplished through its obtained result of 96.28% compared to other models like CAIM with CNN, CAIM with ARIMA and LSTM model.

Figure 8 illustrates the FAR performance for several blockchains with the ML model. The proposed CAIM-based blockchain with LSTM has produced less false rate in the transmitting node request. It determines a better result of 3.72, which is comparatively better compared to other models like CAIM with CNN, CAIM with ARIMA and LSTM model.

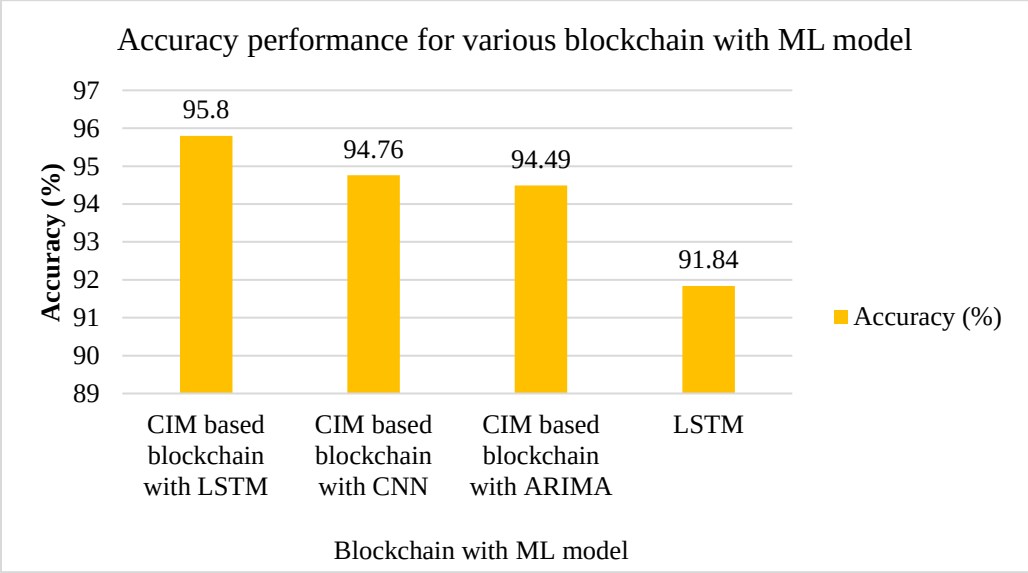

Fig. 6 Accuracy for various blockchains with ML model

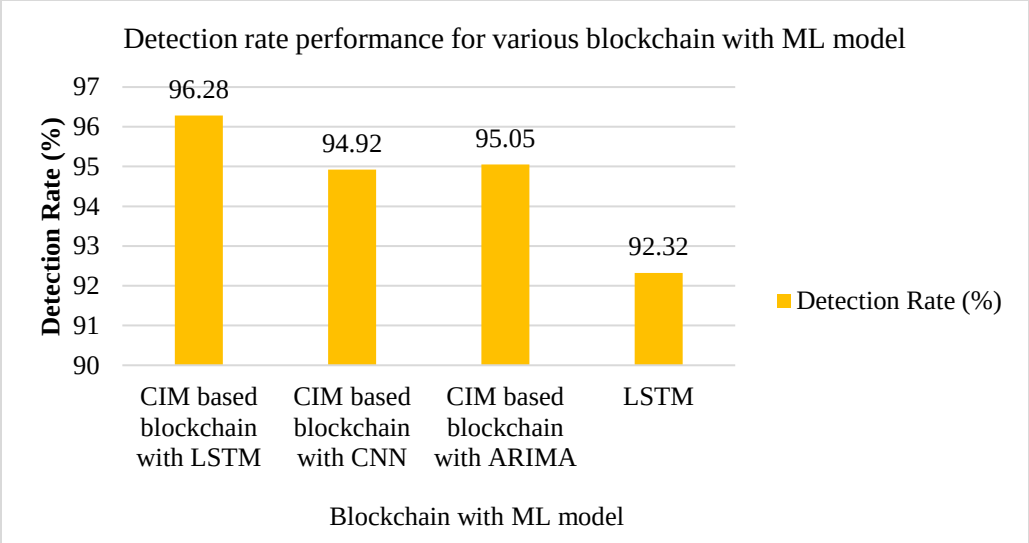

Fig. 7 DR for various blockchains with ML model

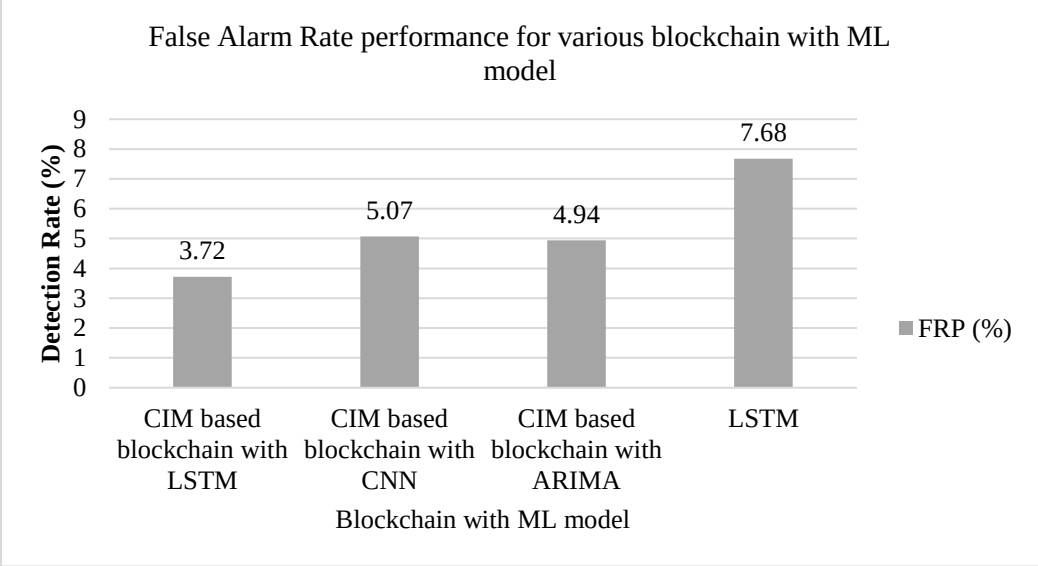

Fig. 8 FAR for various blockchains with ML model

Therefore, blockchain cybersecurity is improved using CAIM, which encased the IDM and LSTM model that produced a better file prediction through PoW as a consensus node in generating a well-secured blockchain model.

5. Conclusion

Recent cyber-attacks have been introduced along with the increase in Internet users. These cyber-attacks significantly affect the performance and security of an entire network. IDMS are employed to prevent these cyber-attacks in which CAIM is introduced in blockchain to minimize the false rate that is a major challenge because of the volume and unreliability of the data. Rapid advancements in deep learning have generated an unfulfilled need for computational technology for blockchain platforms in the Cloud environment. BCN using an IDM model can successfully guarantee data security but at the expense of consuming better processing power. Based on the understanding, the computing demands for training and testing an LSTM model are asymmetric and present a new consensus technique named PoW that directs otherwise wasted blockchain computing to the useful benefits of training LSTM models. Moreover, the designed architecture of the CAIM-based blockchain with the LSTM model has generated better cybersecurity by producing better results in accuracy at 95.80%, DR with 96.28% and less FAR with 3.72 than other CAIM-based models and traditional LSTM models. Therefore, the proposed method is obtained with high cyber security through context-aware.

Reference

[1] Jong-Hyouk Lee, "BiDaaS : Blockchain Based ID As a Service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nicolas Buchmann et al., "Enhancing Breeder Document Long-Term Security Using Blockchain Technology," [CrossRef] [Google Scholar] [Publisher Link]

[3] E. Sweetline Priya, R. Priya, and R. Surendiran, "Implementation of Trust-Based Blood Donation and Transfusion System Using Blockchain Technology," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 104-117, 2022.[CrossRef] [Publisher Link]

[4] Dr. I.Lakshmi, "A Study on the Internet of Things and Cyber Security with Intruders and Attacks," *International Journal of P2P Network Trends and Technology*, vol. 9, no. 3, pp. 4-13, 2019. [Publisher Link]

[5] Benjamin Leiding, and Alex Norta, "Mapping Requirements Specifications Into a Formalized Blockchain-Enabled Authentication Protocol for Secured Personal Identity Assurance," *Future Data and Security Engineering*, pp. 181-196, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hasnae L'Amrani et al., "Identity Management Systems: Laws of Identity for Models0 Evaluation," *In Proceedings of the 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco*, pp. 736-740, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yang Liu et al., "Blockchain-Based Identity Management Systems: A Review," *Journal of Network and Computer Applications*, vol. 166, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] A. Shobanadevi et al., "Novel Identity Management System Using Smart Blockchain Technology," *International Journal of System Assurance Engineering and Management*, vol. 13, pp. 496–505, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] M.Sharada Varalakshmi, "A Case Study of Criticality Based Access Control in a Cyber Physical System," *International Journal of P2P Network Trends and Technology*, vol. 7, no. 5, pp. 41-43, 2017. [Publisher Link]

[10] Mauro Conti et al., "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials* vol. 20, no. 4, pp. 3416–3452, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Kamal Benzekki et al., "A Context-Aware Authentication System for Mobile Cloud Computing." *Procedia Computer Science*, vol. 127, pp. 379-387, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Sagheer Abbas et al., "Modeling, Simulation and Optimization of Power Plant Energy Sustainability for Iot Enabled Smart Cities Empowered with Deep Extreme Learning Machine," *IEEE Access*, vol. 8, pp. 39982–97, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Chibuike Ndubuisi Nwoke et al., "Determinants of Cybercrime Awareness Among Internet Users In Nigeria," *SSRG International Journal of Humanities and Social Science*, vol. 8, no. 5, pp. 14-22, 2021. [CrossRef] [Publisher Link]

[14] Dr.S.Kannan, and Mr.T.Pushparaj, "Creation of Testbed Security Using Cyber-Attacks," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 11, pp. 4-14, 2017. [CrossRef] [Publisher Link]

[15] Bhabendu Kumar Mohanta et al., "Blockchain Technology: A Survey on Applications and Security Privacy Challenges," *Internet of Things*, vol. 8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Andreas Grüner, Alexander Mühle, and Christoph Meinel, "ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider," *IEEE Access*, vol. 9, pp. 138553–138570, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sreedharan, S., and Rakesh, N, "Securitization of Smart Home Network Using Dynamic Authentication," *International Conference on Computer Networks and Communication Technologies*, pp. 287–293, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Neha Priya, "Cybersecurity Considerations for Industrial IoT in Critical Infrastructure Sector," *International Journal of Computer and Organization Trends*, vol. 12, no. 1, pp. 27-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Evans Mwasiaji, and Kenneth Iloka, "Cyber Security Concerns and Competitiveness for Selected Medium Scale Manufacturing Enterprises in the Context of Covid-19 Pandemic in Kenya," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 8, pp. 1-7, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Seyed Mehdi Hazrati Fard , and Sattar Hashemi, "Sparse Representation Using Deep Learning to Classify Multi-Class Complex Data," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, pp. 637–647, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Abdelhakim Zeroual et al., "Deep Authentication Model In Mobile Cloud Computing," *In Proceedings of the 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1-4, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Mohammed Abuhamad, "Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors," *IEEE Internet Things Journal*, vol. 7, no. 6, 5008–5020, 2020. [CrossRef] [Publisher Link]

[23] Kun Xia, Jianguang Huang, and Hanyu Wang, “LSTM-CNN Architecture for Human Activity Recognition,” *IEEE Access*, vol. 8, pp. 56855–56866, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mohammed Amine Bouras et al., “A Lightweight Blockchain-Based Iot Identity Management Approach,” *Future Internet*, vol. 13, no. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Vencelin Gino V, and Amit KR Ghosh, "Enhancing Cyber Security Measures for Online Learning Platforms," SSRG *International Journal of Computer Science and Engineering*, vol. 8, no. 11, pp. 1-5, 2021. [CrossRef] [Publisher Link]

[26] Lukas Stockburger et al., “Blockchain-Enabled Decentralized Identity Management: the Case of Self-Sovereign Identity in Public Transportation,” *Blockchain: Research and Applications*, vol. 2, no. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Preetha S, Sagar J, and Krishna Pooja P, "Security Issues Faced by Internet of Things: A Survey," *International Journal of Recent Engineering Science*, vol. 7, no. 3, pp. 1-6, 2020. [CrossRef] [Publisher Link]

[28] Xinyin Xiang et al., “Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems,” *IEEE Access*, vol. 8, pp. 171771–171783, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Shangping Wang, Ru Pei, and Yaling Zhang, “EIDM: A Ethereum-Based Cloud User Identity Management Protocol,” *IEEE Access*, vol. 7, pp. 115281– 115291, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Iván Gutiérrez-Agüero et al., “Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum,” *IEEE Access*, vol. 9, pp. 108912–108923, 2021. [CrossRef] [Google Scholar] [Publisher Link]