Hindawi
Security and Communication Networks
Volume 2023, Article ID 9861017, 1 page
https://doi.org/10.1155/2023/9861017

Retraction

Retracted: Blockchain Integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Sanober, M. Aldawsari, A. D. Karimovna, and I. Ofori, "Blockchain Integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks," *Security and Communication Networks*, vol. 2022, Article ID 8649060, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8649060, 9 pages
https://doi.org/10.1155/2022/8649060

Research Article

Blockchain Integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks

Sumaya Sanober,[1] **Mohammed Aldawsari**,[2] **Abdurakhimova Dilora Karimovna**,[3] **and Isaac Ofori**[4]

[1]*Prince Sattam Bin Abdul Aziz University, Wadi Aldwassir 1191, Saudi Arabia*
[2]*Department of Computer Science, College of Arts and Science, Prince Sattam Bin Abdul Aziz University, Saudi Arabia*
[3]*Department of Corporate Finance and Securities, Tashkent Institute of Finance, Tashkent, Uzbekistan*
[4]*Department of Environmental and Safety Engineering, University of Mines and Technology, Tarkwa, Ghana*

Correspondence should be addressed to Isaac Ofori; iofori@umat.edu.gh

Received 20 May 2022; Revised 1 July 2022; Accepted 14 July 2022; Published 10 August 2022

Academic Editor: Mukesh Soni

Digitalization of financial institutes, industries, and organizations to provide fast online services needs a large number of Internet connections and different types of networks. The presence of a large number of digital networks makes operational communication and data transfer vulnerable to different cyber-attacks. So, to secure the system, there must be a mechanism present to detect malicious activities and give an alarm to the operator/HMI. A numerous intrusion detection system is present in this era but still, the intruders get access to the network and create an economical loss. Blockchain is a new path to gain the trust in the cybersecurity field. Researchers have been working on the term "blockchain technology" for the past few years. In a growing digital environment, blockchain is a novel technology that provides various advantages. This paper identifies and examines the possible way to enhance the blockchain capability by integrating with principal component analysis (PCA). The bad data are removed from the real-time data set and then pass through the blockchain mechanism to identify the threats. The results of the investigation and analysis demonstrate that, when compared to the traditional approach, the PCA integration with the blockchain method proposed in this paper may reduce detection time and boost detection rate.

1. Introduction

Due to the increased use and reliance on network-connected platforms and internet-connected gadgets, government agencies and sectors are becoming increasingly vulnerable to cyber-attacks [1]. Network attacks are unauthorized activities against digital assets within an organization's network. Malicious actors frequently utilize network attacks to manipulate, remove, or steal sensitive data. Attackers on networks typically target network perimeters in order to gain access to internal systems [2, 3]. Network attacks are classified as either passive or aggressive. Malicious actors get unauthorized network access, monitor, and steal sensitive data without making any modifications in passive network attacks. Active network assaults include data modification, encryption, and destruction [4, 5]. Advanced hackers can get unauthorized access by bypassing speech recognition, retinal scans, and access codes. They just need to break the system's firewall to fool the biometric system. Furthermore, keeping data in a limited space makes it easier for hackers to swiftly steal the data and utilize it to their advantage. Hackers frequently attack your system in stages, and it is simple to erase any evidence of their first infiltration. As a result, not only must safe cyber systems be in place but also measures must be in place to detect cyber security assaults in a timely manner. Through analysis by using the organization logs present in the network system, the system security architecture can be identified [6]. Even if the fight against cyber threats and attacks is never over, it is feasible to avoid them by understanding the many protocols, vulnerabilities,

resources, and tools that criminal actors employ. Furthermore, by predicting attacks and knowing where to search for them, you may construct defenses for your systems. Antivirus software and endpoint security services provide value for money by protecting your network against viruses and brute force attempts to access your computers. To recognize and respond to known attack code, malware defenses must be set up and maintained. Patch management, which entails patching known vulnerabilities with the most recent version of the device, is used to prevent attacks that exploit software defects. Every year, new and updated threats are used to gain access to the system due to the need for an advanced intrusion detection system that can be upgraded and detect new threats [7, 8]. Cyber security solutions are technological tools and services that help businesses protect themselves against cyber-attacks, which can result in application downtime, data theft [9], reputational damage [10], adherence penalties, and other undesirable consequences [11, 12]. IoT security aids in the establishment of insight and the application of security controls to the expanding network of IoT devices, which are increasingly used for mission-critical applications and store sensitive data but are often meant to be insecure. Cloud security aids in obtaining control of complex public, private, and hybrid cloud systems by detecting and correcting security misconfigurations and flaws [13, 14].

Blockchain is revolutionizing the organization, which can change the intrusion detection system by providing more innovative and advanced solutions [8]. The rise of blockchain started with the rise of cryptocurrency, but with various studies, it has been found that it can have better applications in different sectors also. In worldwide industry and organization, it has been used to tackle financial-based cyber threats [15]. In the last few years, the blockchain technology has been evolving so much that it has surpassed the main purpose and has been used for different sectors. Most importantly, the blockchain may allow a new breed of decentralized apps without middlemen and serve as the cornerstone for critical components of Internet security infrastructures [16]. By identifying and avoiding data tampering, artificial intelligence (AI) might be utilized to improve the process of establishing blockchains. Furthermore, AI built to protect a system or database may be implemented as a blockchain application that does not rely on the integrity of trusted nodes [17, 18]. Many DDoS attacks make advantage of domain name servers (DNS), which convert IP addresses into human-readable website names. When DNS is shifted to the blockchain, resources may be shared among several nodes, making it difficult for attackers to control the database [19, 20]. As a result, finding current research on the application of blockchain to the problem of cyber security is vital in order to comprehend how evolving technologies might assist mitigate growing threats.

With respect to different literature reviews in [21, 22], very few progress has been done in cyber security in an industrial application using blockchain. In one of the recent research works [23, 24], the author highlights different perspectives of blockchain its advantages, disadvantages, and challenges [25, 26]. Few authors highlight the authentication mechanism that can be used by different industries and organizations through the blockchain model. Any industry's cyber physical architecture (CPA) relies on a dependable and timely interaction between the cyber and physical layers, which can be split into three categories as follows: normal monitoring: in the event of an unhealthy operation in the CPA, this form of communication does not necessitate rapid intervention. The monitoring time ranges from milliseconds to fractions of a second. Closed loop monitoring (CLM): sensors and actuators measure parameters, which are then relayed to a central control room for quick response in the event of an abnormality. Communication times vary between 20 and 200 milliseconds. Interlocking: command is delivered by interlocking for continuous monitoring, operations, and control [27]. This type of communication is delicate, and data must be exchanged within a time range of milliseconds. The emergence of blockchain coincided with the growth of bitcoin, but several researches have revealed that it may be used in a variety of industries. The authors present a blockchain-based authentication technique that may be employed by many industries and organizations. This type of communication does not need immediate intervention in the case of a harmful operation in the CPA. The system security architecture may be recognized by analyzing the organization logs contained in the network system.

We live in a digital era because everything in our digital age has been transferred online. We utilize the Internet to assist us in doing jobs, whether it is data storage or information access. As our involvement in the digital world expands, so does our vulnerability to cyber assaults. For the system to be secure, a mechanism that can detect malicious activities and inform the operator or HMI must be present. To develop a system that ensures secure data is of the greatest importance To enhance the blockchain methodology for better performance, it is integrated with PCA. PCA is used to reduce the dimension of large data set so that it can work on big data system. For security purposes, a system should reduce the data set of historical data and extract the best features from the data set so that it can identify malicious activities through blockchain. The next section introduces the architecture of blockchain and PCA.

2. Architecture of the Proposed Model

This section deals with the details of blockchain, PCA, and its integration for better performance.

2.1. Blockchain Architecture. Blockchain is the new advance approach to security as it stores the data related to transactional which are known as the system block of the network structure in which it is been implemented. The network server's database is called chain which is used to connect one system to other in the network. The storage which stores these data is called a "digital ledger" [28, 29]. Blockchain is ideal for distributing such information because it provides immediate, shareable, and completely transparent data stored on an immutable ledger that can only be accessed by

network members with permission [30, 31]. For each and every transaction inside, the ledger and special digital signature are required. The best part of this process is that the data can be used and visualized by everyone, but it can be tampered with due to this digital signature process. The blockchain has the following main features [32]:

(i) Highly independent and secure: the blockchain uses the digital signature which is the most advanced feature and keeps the fraud activity away. Also, by using this, the transaction among two parties can be done with mutual understanding without involving large steps.

(ii) Immutability capability: the best feature of the blockchain is it cannot be altered. This helps to ensure that technology does not change throughout the process. Every node used in the network has the digital ledger, so for every transaction, each digital ledger should be matched and validated.

(iii) Decentralized: With less involvement of the third party, the system is fast, and less failure rate is faced compared to different advanced technology.

So, from above, it is clear that blockchain can never be modified which helps in the integrity of the system. Figure 1 displays the concept of blockchain interaction. The node in the blockchain can add a new node such that each node added can see the blockchain architecture. Using any of two algorithms, that is, proof of stake and resistant of effort, the novel node can be added. In proof of stake, the new node which is going to be added to the system shows that they own some stake in the previous block, so their participation is valid. Each block contains the details such as former mess, transaction details, and POW/POS information. As shown in Figure 1, each block is connected with each other [33]. The connection is between the previous transaction and the present hash of the block.

The blockchain technology is a combination of the following three main parts:

(i) The secure cryptography keys

(ii) A network work as peer-to-peer having shared ledger details

(iii) Storage place to store the data's

The secure cryptography key consists of the following two keys, the first is the public key and the second is the private key. The sender's address (public key), the receiver's address, the transaction, and his/her private key data are all sent via the SHA256 method. Until being uploaded to the blockchain, the digital information, called as hash decryption, is transported around the world and confirmed [34].

2.2. Principal Component Analysis (PCA) Architecture. The model's complexity grows in tandem with the magnitude of the data. This study employs a novel intelligent dimension reduction approach known as principal component analysis to overcome this issue (PCA), which allows

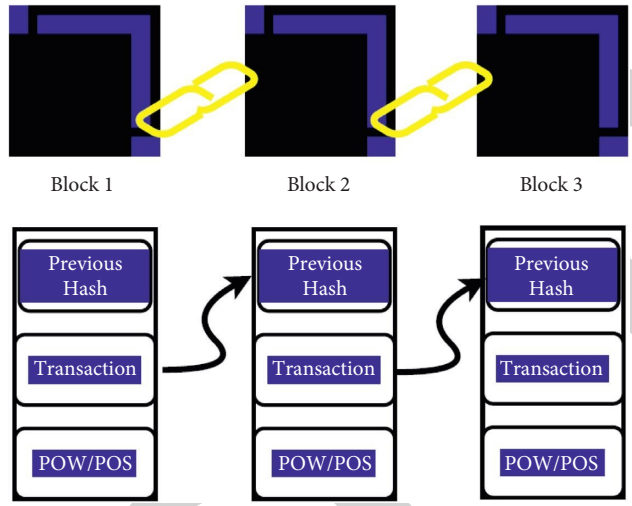

Figure 1: Blockchain architecture.

for data visualisation and the quick extraction of key characteristics that can then be put into an unsupervised machine learning model [35]. This aids in the better visualisation of the dataset as well as its performance. PCA is a method for decreasing the length of datasets while retaining as much information as possible. As a consequence, it extracts a low-dimensional collection of characteristics by lowering dimension by translating a huge dataset into a shorter one with more content retained.

When working with three-dimensional or higher-dimensional data, PCA is more useful. A linear combination of original variables is called PCA. The first principal component was chosen to describe the highest quantity of alteration in the original datasets. The first principal component still contains the most information about the original data [36–38]. The second principal component, which is unrelated to the first and subsequent principal components, attempts to explain the remaining variation in the dataset as shown in Figure 2.

So, to reduce the dimension of the data sets, the following steps are followed [39–41]:

(i) Step 1: this step normalizes the range of continuous starting variables so that they all directly contribute to the study. If the ranges of starting variables differ greatly, the variables with larger ranges will dominate over those with narrower ranges (e.g., a variable ranging from 0 to 100 will prevail over a variable scale from zero to 1), leading to biased results.

(ii) Step 2: the purpose of this step is to determine how the variables in the input data set depart from the mean in respect to one another or to determine if there is a relationship between them. To detect these correlations, we construct the covariance matrix.

(iii) Step 3: the linear algebra concepts of eigenvectors and eigenvalues are what we all want to estimate from the covariance matrix in order to discover the fundamental components of the data.

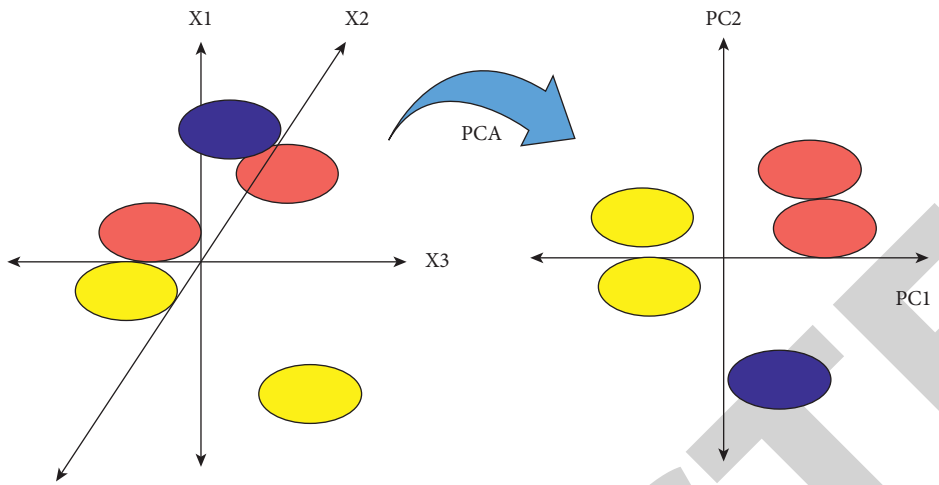

Figure 2: PCA component.

(iv) Step 4: in the last step, eigenvalue is stated in descending order, which helps to find the principal components of the data sets. In this step, elimination of nonsignificant data is done. So the feature vector is obtained. And at the last, the data are arranged in the principal axis.

2.3. Blockchain-Integrated PCA Methodology. This statistical approach uses an orthogonal transformation to convert observations of correlated qualities into a collection of linearly uncorrelated properties. The newly changed qualities are the principal components. It is a well-known tool for exploratory data analysis and predictive modeling. It is a technique for extracting significantly dominant from a dataset by reducing variances. Finally, the erroneous data are removed from the real-time data gathering, and the risks are recognized by utilizing the blockchain system. Combining PCA with blockchain can give more accurate and strong protection against any cyber intrusion. The PCA helps to reduce the dimensions of large data set which can be used by blockchain as real-time data or historical data set. Figure 3 shows how the PCA can be integrated with the blockchain system to enhance the security feature of the new methodology. It consists of two main points. The first is key matching, and the second is the extraction of feature using PCA.

If PCA is not present, then the blockchain has to deal with the big data sets which make the system a little sluggish. The sluggish system will face lots of failure rates. Now, in the next section, we will see how this proposed methodology can prove to be the best.

3. Results and Discussion

This section highlights the advantages of the PCA-integrated blockchain method for cyber security using the statistical data obtained through an extensive literature survey used in the introduction section.

3.1. Results. Using blockchain in different work profiles is shown in Figure 4. It can be seen that from cryptocurrency, now the most use of blockchain is in the field of IoT-based sectors [42–44]. So, it can be seen that both PCA and blockchain have almost the same kind of uses as per the requirement, also shown in Figure 5.

The research over the time period of 10 years on the topic PCA and blockchain is shown in Figure 6. Each year, the related research has been increased in many folds. Now, we will use simulation to see how the PCA affects the working of blockchain methodology when large data sets are present in the system.

Figure 7 shows the speed and accuracy of blockchain when working alone on different large data sets. The sample of data sets was of multiple of 10 so it started from 10 K (10000) datasets, and it went up to 100000 K. It can be seen that as the data set quantities were increasing, the speed of working increased rapidly. Now, in the same system when integrated with the PCA, the results are somewhat more better compared to blockchain working alone. In Figure 8, it shows that even if the data set is increasing in many folds but then also the speed of working of the proposed methodology is somewhat constant and has a very small value in milliseconds.

Now, after comparing the results based on datasets, speed, and accuracy, it has time to compare the system on basis of storage cost requirements. Storage cost means that the total cost required to store the data is coming from different sources. From Figure 9, it is clear that the data storage cost saving is more when blockchain is integrated with PCA. PCA is used to reduce the size of a data set and extract future value that can be utilised to recreate the original data. As it can be seen, both PCA and blockchain have nearly identical purposes in terms of requirements, and associated research is growing at a rapid pace. It can be observed that as the size of the data collection grows, so does the speed with which it is processed. When the same system is used with the PCA, the results are somewhat better than when blockchain is used alone. The entire cost of storing data from various sources is referred to as storage cost.

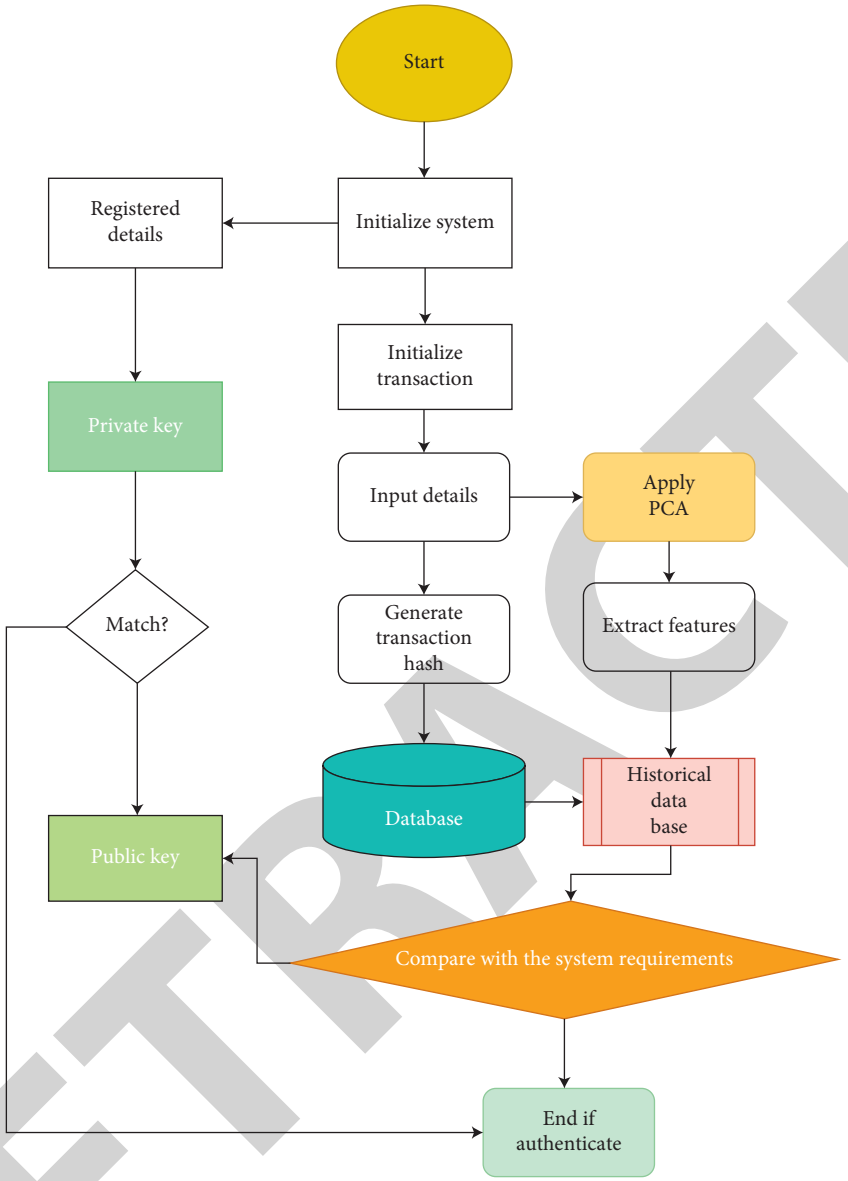

Figure 3: Proposed PCA Blockchain integration.

3.2. Discussion. To keep various organizations out of the news, one must understand the most common causes of data breaches including what you can do to mitigate the dangers they offer. For the system to be secure, a mechanism that can detect malicious activities and inform the operator or HMI must be present. Despite the numerous intrusion detection technologies in use today, hackers continue to breach networks and cause financial damage. Combining PCA with blockchain may give a much more precise and strong defense against any cyber intrusion. In today's world, blockchain technology continues to evolve and find new uses. One of the possible places where it has been investigated and used is cyber security. Still, more research is needed to make it possible to use in the real-time scenario of cyber security or for the intrusion detection technique. Although this paper highlights a new approach that can be used for the future intrusion detection architecture, there are still few problems that exist and need to be workout in the future. Blockchain has many future scopes as stated as follows:

(i) Blockchain with PCA can be used in the digital financial sector where a large number of datasets are present

(ii) A major security area is still prone to large cyberattack which can be reduced by involving blockchain with PCA

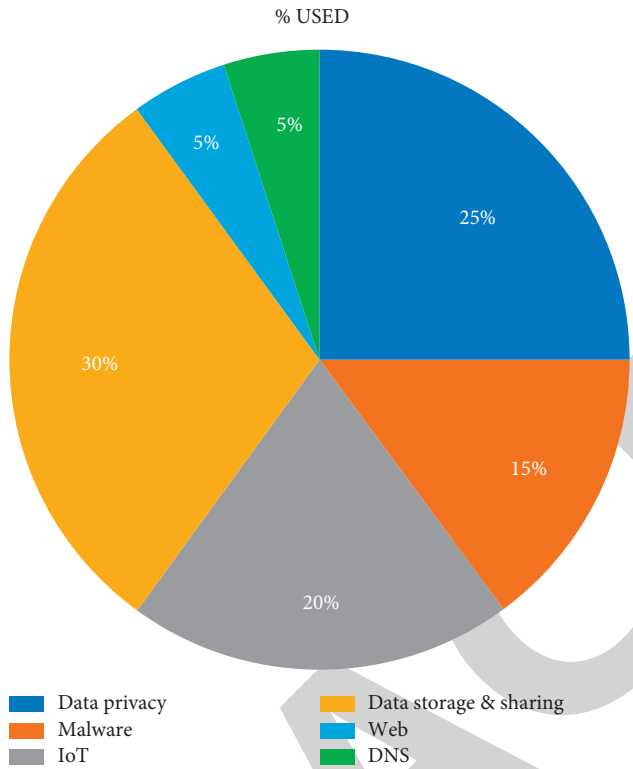

Figure 4: Blockchain main uses.

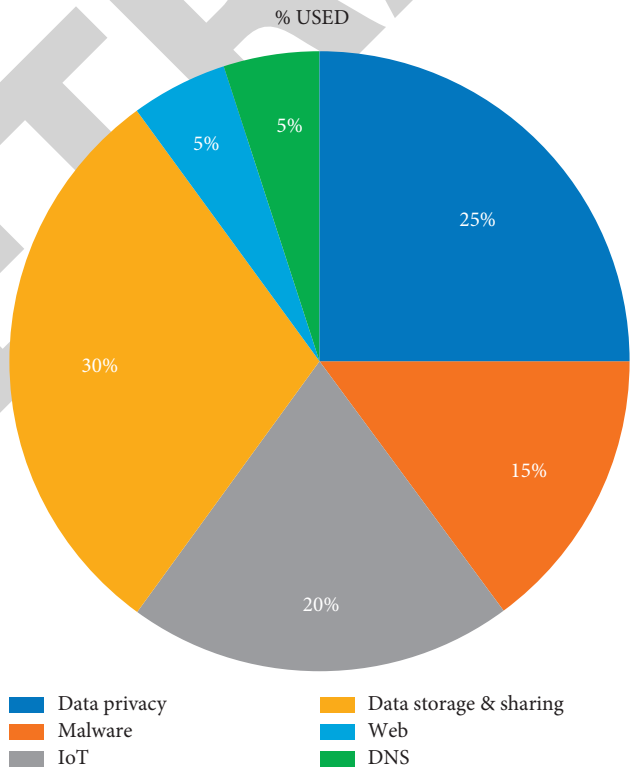

Figure 5: Use of PCA in different sectors.

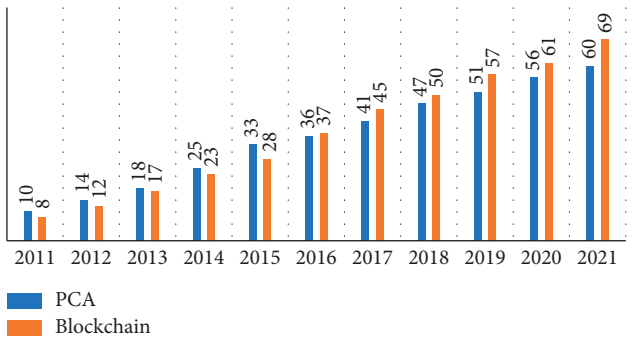

Figure 6: Year-wise research on the topic of PCA and blockchain.

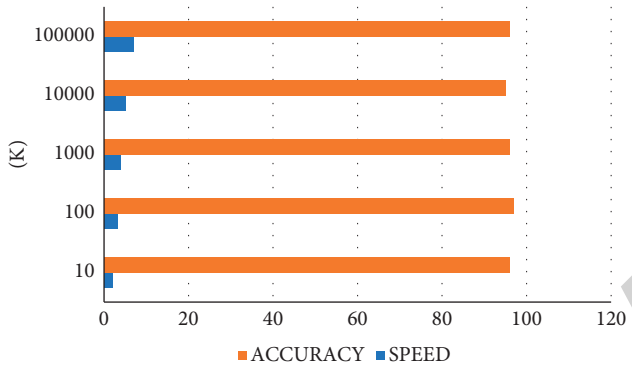

Figure 7: Blockchain speed and accuracy with different datasets.

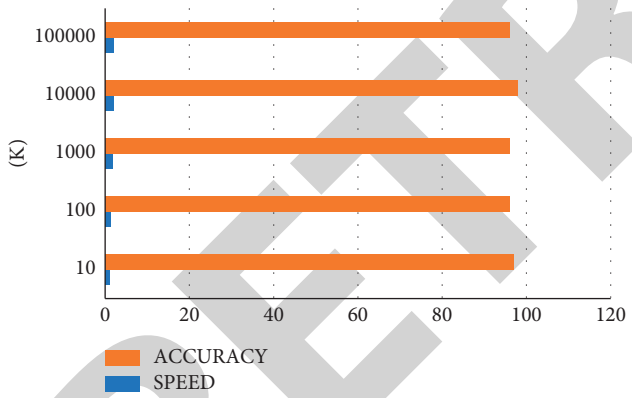

Figure 8: Blockchain integrated with PCA.

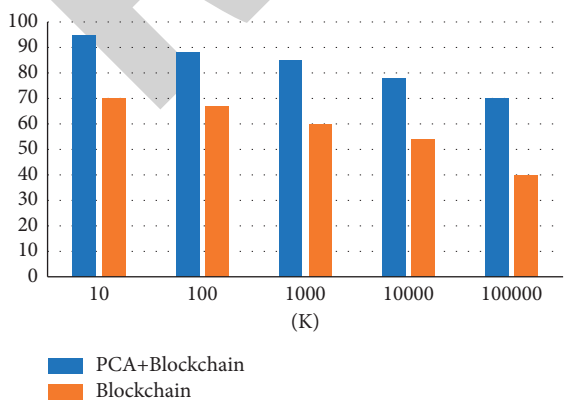

Figure 9: Storage cost saving.

4. Conclusion

The article analysed the application of the blockchain technique from the viewpoints of many investigators that published their research articles. The majority of blockchain safety specialists seem to be concentrating their efforts on IoT device acceptance. The safety of blockchain also includes networks and data. Blockchain technology, as mentioned in the conversation, can be utilized to safeguard IoT devices by providing more trustworthy confirmation and data transfer procedures. Network latency to run the distributed network was frequently mentioned in the study on IoT security using blockchain applications. Because of the variety in results used by all sets of scientists, it was not possible to quantify such data for the purposes of this work. A future study might include assessing network latency, energy usage, and data packet fluxes in blockchain-based IoT networks, as well as standardising data presented in basic research.

Finally, blockchain can safeguard data throughout storage and transmission by encoding blocks that can only be accessed by sender and receiver and cannot be tampered with. Future researchers should look at the potential of using a single blockchain to build information security, like most current options use several blockchains, rendering integration challenges.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: the foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[2] G. S. Sriram, "Resolving security and data concerns in cloud computing by utilizing a decentralized cloud computing option," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1269–1273, 2022.

[3] S. A. Patel, S. P. Patel, Y. B. K. Adhyaru, S. Maheshwari, P. Kumar, and M. Soni, "Developing smart devices with automated Machine learning Approach: a review," *Materials Today Proceedings*, vol. 51, pp. 826–831, 2022.

[4] H. Li, M. Shabaz, and R. Castillejo Melgarejo, "Implementation of python data in online translation crawler website design," *International Journal of System Assurance Engineering and Management*, 2021.

[5] B. Prasanalakshmi, K. Murugan, K. Srinivasan, S. Shridevi, S. Shamsudheen, and Y. C. Hu, "Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography," *The Journal of Supercomputing*, vol. 78, no. 1, pp. 361–378, 2022.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the 2017 IEEE International*

Congress on Big Data (BigData Congress), pp. 557–564, IEEE, Honolulu HI USA, June 2017.

[7] V. Jagota and R. K. Sharma, "Wear volume prediction of AISI H13 die steel using response surface methodology and artificial neural network," *Journal of Mechanical Engineering and Sciences*, vol. 14, no. 2, pp. 6789–6800, 2020.

[8] G. Wood, *Ethereum: A Secure Decentralized Generalized Transaction Ledger Yellow Paper*, Ethereum Project. Yellow Pap, Etherum, Zug, Switzerland, 2014.

[9] V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*Etherum, Zug, Switzerland, 2014.

[10] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc, Sebastopol, CA, USA, 2015.

[11] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc, Sebastopol, CA, USA, 1 edition, 2015.

[12] A. Shobanadevi, S. Tharewal, M. Soni, D. D. Kumar, I. R. Khan, and P. Kumar, "Novel identity management system using smart blockchain technology," *International Journal of System Assurance Engineering and Management*, vol. 13, no. S1, pp. 496–505, 2022.

[13] G. K. Saini, H. Chouhan, S. Kori et al., "Recognition of human sentiment from image using machine learning," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 5, pp. 1802–1808, 2021.

[14] J. Bhola, M. Shabaz, G. Dhiman, S. Vimal, P. Subbulakshmi, and S. K. Soni, "Performance evaluation of multilayer clustering network using distributed energy efficient clustering with enhanced threshold protocol," *Wireless Personal Communication*, 2021.

[15] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[16] M. Crosby, P Pradan, V. Sanjeev, and K. Vignesh, "Blockchain technology: beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[17] G. S. Sriram, "Security challenges of big data computing," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1164–1171, 2022.

[18] M. Yang, P. Kumar, J. Bhola, and M. Shabaz, "Development of image recognition software based on artificial intelligence algorithm for the efficient sorting of apple fruit," *International Journal of System Assurance Engineering and Management*, vol. 13, no. 5, pp. 322–330, 2021.

[19] F. Ajaz, M. Naseem, S. Sharma, M. Shabaz, and G. Dhiman, "COVID-19 challenges and its technological solutions using IoT," *Current Medical Imaging Formerly: Current Medical Imaging Reviews*, vol. 18, no. 2, pp. 113–123, 2022.

[20] D. Y. Jiang, H. Zhang, H. Kumar et al., "Automatic control model of power information system Access based on artificial intelligence technology," *Mathematical Problems in Engineering*, vol. 2022, Article ID 5677634, 6 pages, 2022.

[21] C. Cachin, "Architecture of the hyperledger blockchain fabric," *InWorkshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 1, p. 4, 2016.

[22] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018.

[23] W. Li, S. Andreina, J. M. Bohli, G. Karame, "Securing proof-of-stake blockchain protocols," *Lecture Notes in Computer Science*, Springer, New York, NY, USA, 2017.

[24] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science - Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[25] S. Chen, C. Y.-H. Chen, W. K. Hrdle, T. M. Lee, and B. Ong, "Chapter 8 – Econometric Analysis of a Cryptocurrency Index for Portfolio Investment BT," *Handbook o Blockchain, Digital Finance, and Inclusion*, Academic Press, Cambridge, MA, USA, 2018.

[26] K.-K. R. Choo, "Cryptocurrency and virtual currency," in *Handbook of Digital Currency*Elsevier, Amsterdam, Netherlands, Article ID 283307, 2015.

[27] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, "Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence," *IEEE Trans. Emerg. Top. Comput.*, < >, vol. 8, no. 2, pp. 341–351, 2017.

[28] O. Osanaiye, H. Cai, K.-K. R. Choo, A. Dehghantanha, Z. Xu, and M. Dlodlo, "Ensemblebased multi-filter feature selection method for DDoS detection in cloud computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 130, 2016.

[29] "Five ways banks are using blockchain," 2022, https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b.

[30] G. Murugesan, T. I. Ahmed, M. Shabaz et al., "Assessment of mental workload by visual motor activity among control group and patient suffering from depressive disorder," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 8555489, 10 pages, 2022.

[31] K. Jairath, N. Singh, M. Shabaz, V. Jagota, and B. K. Singh, "Performance Analysis of Metamaterial-Inspired Structure Loaded Antennas for Narrow Range Wireless Communication," *Scientific Programming*, vol. 2022, Article ID 7940319, 17 pages, 2022.

[32] "How blockchain will transform the supply chain and logistics industry," 2018, https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/?sh=45cf92ab5fec.

[33] K. Megget, "Securing the supply chain," 2018, https://www.accenture.com/us-en/insights/consulting/securing-the-supply-chain.

[34] R. M. Parizi, Amritraj, and A. Dehghantanha, "Smart contract programming languages on blockchains: an empirical evaluation of usability and security," in *Proceedings of the International Confernce on Blockchain*, pp. 75–91, Springer, Seattle, USA, June 2018.

[35] "Smart contracts on the blockchain: can businesses reap the benefits," 2017, https://www.forbes.com/sites/rogeraitken/2017/11/21/smart-contracts-on-the-blockchain-can-businesses-reap-the-benefits/?sh=51a2019d1074.

[36] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[37] "Convergence of blockchain and cybersecurity - IBM government industry blog," 2020, https://www.ibm.com/blogs/blockchain/category/blockchain-for-government/page/2/.

[38] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?-A systematic review," *PLoS One*, vol. 11, no. 10, Article ID e0163477, 2016.

[39] M. Conoscenti, A. Vetr, and J. C. De Martin, "Blockchain for the internet of things: a systematic literature review," in *Proceedings of the 2016 IEEE/ACS 13th International*

Conference of Computer Systems and Applications (AICCSA), pp. 1–6, IEEE, Agadir, Morocco, November 2016.

[40] S. Seebacher and R. Schritz, "Blockchain technology as an enabler of service systems: a structured literature review," in *Exploring Services Science*, pp. 12–23, Springer, New York, NY, USA, 2017.

[41] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," *Engineering*, vol. 2, p. 1051, 2007.

[42] S. Saralch, V. Jagota, D. Pathak, and V. Singh, "Response surface methodology based analysis of the impact of nanoclay addition on the wear resistance of polypropylene," *The European Physical Journal - Applied Physics*, vol. 86, no. 1, Article ID 10401, 2019.

[43] S. Hosseini, B. Turhan, and D. Gunarathna, "A systematic literature review and meta-analysis on cross project defect prediction," *IEEE Transactions on Software Engineering*, vol. 45, no. 2, pp. 111–147, 2019.

[44] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.