IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 10, October 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

Creation of an Anomaly Detection System for Blockchain-based Cloud Deployments that Consider Privacy and Delay

Mala K, Manasa U

Assistant Professor, Department of ISE, CIT, Gubbi, Tumkur, Karnataka, India

UG Student, Department of ISE, CIT, Gubbi, Tumkur, Karnataka, India

ABSTRACT: Cloud-based deployments are increasingly vulnerable to many kinds of assaults; hence powerful anomaly detection systems are needed to prevent security breaches. While effective to some degree, current methods like RSSI, GTM, and APG have drawbacks in terms of scalability, precision, and accuracy. In order to improve the forecast accuracy of cloud assaults and optimize blockchain-based cloud installations, this study suggests a novel anomaly detection system that combines multimodal feature analysis, deep learning models, and QoS-aware sidechains. The suggested strategy considerably surpasses traditional approaches in terms of precision, accuracy, recall, and AUC performance by optimizing feature variance across various sample types and utilizing cutting-edge deep learning algorithms. Additionally, the framework shows increased efficiency in terms of throughput, energy usage, and block mining latency, makingcombining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), the system analyses system logs to find anomalous patterns of activity linked to various threats. The architecture guarantees the transparency and integrity of system records through the use of Blockchain technology, while Deep Learning models offer accurate and quick anomaly detection. The advantages of both Deep Learning and Blockchain technology support the choice to merge them. Blockchain technology ensures the accuracy of anomaly detection and prevents tampering with system records by providing a distributed, immutable ledger. On the other hand, deep learning models produce high precision, accuracy, recall, and AUC measures because of their remarkable pattern recognition skills and ability to adjust to shifting attack strategies. Experimental data analyses show the effectiveness of the suggested framework.

KEYWORDS: Anomaly detection, attacks, blockchain, cloud computing, deep learning, privacy.

I. INTRODUCTION

The storage, processing, and access of data by enterprises has been completely transformed by cloud computing, which offers flexible, scalable, and affordable options. However,the increasing dependence on cloud-based installations has given rise to serious security issues. Because cloud settings are dynamic and dispersed, they are vulnerable to a wide range of cyber threats, including as Man-in-the-Middle (MITM), Finney, Sybil, dispersed Denial of Service (DDoS), and Cryptojacking assaults. These assaults have the potential to jeopardize the confidentiality, availability, and integrity of cloud-basedsystems, resulting in severe repercussions for organizations and users.Effective anomaly detection frameworks that can recognize and stop such attacks in cloud deployments are crucial to addressing these security challenges . Furthermore, in order to protect sensitive user datasets and samples.In order to address delay and privacy awareness in blockchain-based cloud deployments, this article presents a novel anomaly detection system that offers strong defences against the aforementioned assaults.There are a lot of important applications for our work when it comes to protecting cloud computing infrastructures. The methodology can be applied in many different contexts, such as corporate deployments of private clouds and enterprise use of public cloud services. The framework protects the integrity and transparency of system logs by fusing blockchain technology with mechanisms for detecting anomalies, which stops tampering and unauthorized modifications. Furthermore, the overall security posture of cloud installations is strengthened by the accurate and prompt detection of anomalies made possible by the application of deep learning algorithms.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

II. LITERATURE SURVEY

The existing approaches for blockchain-based cloud deployment anomaly detection that consider delay and privacy have significantly improved the security and integrity of cloud computing environments. These models detect and block attacks such as Man-in-the-Middle (MITM), Finney, Sybil, Distributed Denial-of-Service (DDoS), and Cryptojacking using a range of approaches and strategies. The goal of this article is to give an overview of prominent modern models and their salient features, such as the effective metric for anomaly analysis provided by the Received Signal Strength Indicator (RSSI).Using machine learning techniques, especially deep learning algorithms, is a common approach in anomaly detection models . Two varieties of deep learning models, namely Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), have demonstrated remarkable efficacy in recognizing patterns and detecting irregularities in system logs and events. These models are perfect for identifying unusual behaviour in cloud installations because they effectively capture intricate linkages and temporal dependencies. Another important aspect of the models under evaluation is the integration of blockchain technology through the Game Theoretic Model (GTM) process. The decentralized, unchangeable ledger of the blockchain enhances the precision and availability of event and system records. The models can ensure the accuracy and tamper-resistance characteristics of the anomaly detection process by integrating blockchain into the frameworks . Furthermore, the blockchain technology process's distributed consensus mechanisms and smart contracts can be used to make system log auditing visible and safe.To protect privacy in cloud environments, collaborative intrusion detection systems have also been researched . These systems use federated learning techniques, which produce an enhanced global model process by training models separately on separate cloud instances and sharing only aggregated updates. Since no instance of the system is needed to exchange data with a central authority or with certain other cases & scenarios, this method allows anomaly detection without jeopardizing the privacy of sensitive data.

III.METHODOLOGY

There are numerous crucial steps in the process for implementing an anomaly detection system in blockchain-based cloud deployments. The first step is data collecting, which includes the ongoing monitoring and collection of blockchain, cloud, and user activity records. The next step is feature extraction and preprocessing, which involves analysing and converting pertinent features—like transaction kinds, data access patterns, and network behaviour—into an analysis-ready format. Then, for anomaly identification, deep learning or machine learning models are used. These models can identify departures from typical behaviour patterns using supervised, unsupervised, or hybrid learning techniques. Since zero-day attacks are unexpected, unsupervised methods like clustering or autoencoders are frequently preferred. In order to confirm and track any discovered irregularities, the system also makes advantage of blockchain's intrinsic transparency and immutability, which guarantees that any unauthorized or questionable activity may be documented in a decentralized, impenetrable way. Over time, feedback loops and ongoing model upgrades aid in improving detection accuracy. Lastly, the system has alerting methods to let administrators know when abnormalities are found, enabling prompt action and possible threat mitigation.Features are recovered from the pre-processed cloud logs by utilizing the capabilities of Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Auto Encoders (AE). These deep learning models are perfect for examining intricate log patterns because they are excellent at identifying latent representations and temporal correlations in sequential data.Sequential dependencies and temporal trends in the log data are captured by LSTM and GRU models, while Auto Encoders (AE) help develop compact representations of input characteristics, efficiently lowering dimensionality and identifying prominent features.

DESIGN OF THE DEEP LEARNING MODEL FOR THE IDENTIFICATION OF UNUSUAL BEHAVIOR PATTERNS.

The suggested deep learning model transforms cloud logs into multidimensional feature sets by combining LSTM, GRU, and Auto Encoders (AEs). IP addresses, ports, protocols, timestamps, HTTP methods, resource access details, device information, CPU/memory utilization, network traffic, database queries, and security events like firewall and intrusion detection system warnings are among the important factors included in these logs. In cloud environments, these properties are essential for spotting irregularities and spotting assaults. For precise anomaly detection, every metric helps analyse odd activities.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

AUTHENTICATION METHOD, AUTHENTICATION SUCCESS/FAILURE, SESSION ID, AND SESSION DURATION.

Unauthorized access attempts, questionable logon behaviour, and session hijacking can be detected by keeping an eye on authentication techniques, success/failure rates, session IDs, and session duration. These settings offer information about session management and user authentication.

SOURCE PORT AND DESTINATION PORT

Determine which network services are involved. Keeping an eye on them aids in identifying odd port usage or unexpected connections that could indicate possible threats.

TIMESTAMP:

Records the date and time of an event, enabling event organization, sequencing, and correlation for analysis.

PROTOCOL

This parameter specifies the network protocol used during a communication session, such as TCP or UDP. Protocol analysis can disclose uncommon or unauthorized protocol usage. These parameters designate the user affiliated with an activity or event. By monitoring user activity, anomalies such as attempts at unauthorized access or suspicious behaviour can be identified.

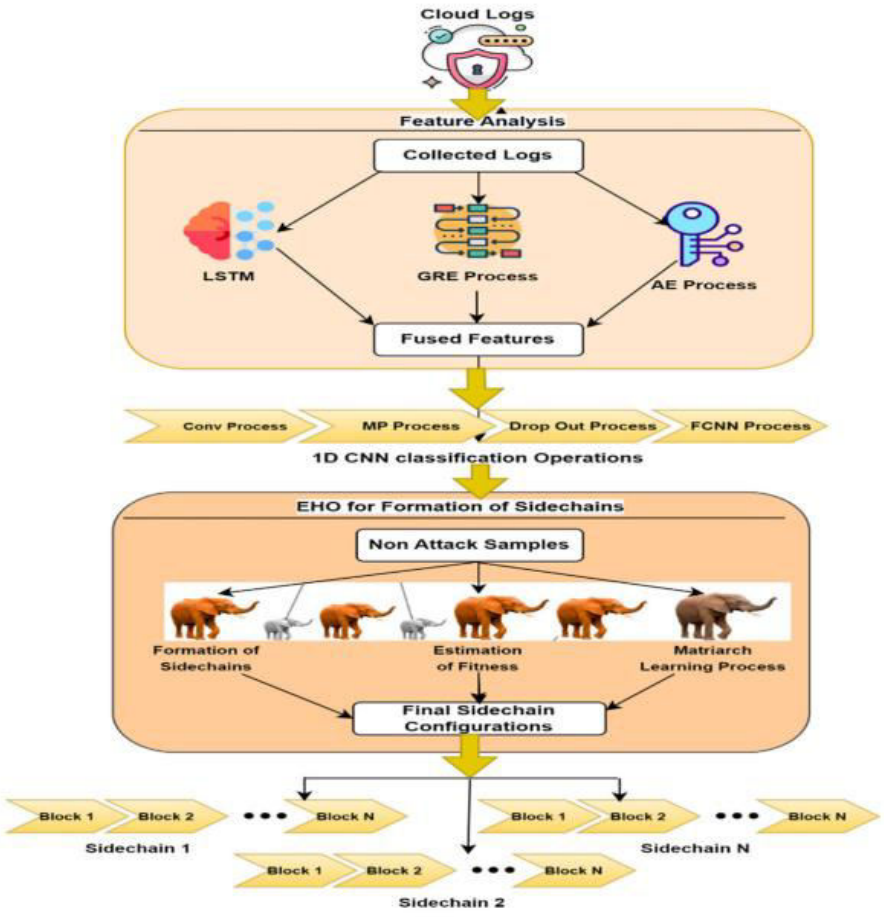

Figure 1:Design of the proposed security model for blockchain-based cloud deployment.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

IV. EXPERMENTAL SETUP AND RESULTS

The anomaly detection framework was implemented on a powerful hardware configuration featuring an Intel Core i7-10700K CPU clocked at 3.80GHz, supported by 32GB of DDR4 RAM. For storage, a 1TB NV Me SSD was utilized, ensuring fast data retrieval and processing speeds. The graphical performance was handled by an NVIDIA GeForce RTX 3080 GPU, allowing for accelerated computation, particularly useful for deep learning model training and large-scale data analysis.

Python 3.9.5 was selected as the primary programming language for its versatility and extensive libraries suited to machine learning and data science. Libraries like TensorFlow and PyTorch were pivotal in building and training deep learning models, while Pandas and NumPy were essential for data preprocessing and analysis, enabling efficient handling of the large datasets.

The framework leverages multiple deep learning algorithms: Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) networks for sequential data analysis, Auto Encoder (AE) for unsupervised feature learning, and 1D Convolutional Neural Network (CNN) for pattern recognition, forming a robust algorithmic approach for anomaly detection.

The dataset comprises log data from cloud platforms and intrusion detection sources. AWS CloudTrail logs (500,000 entries), Microsoft Azure activity logs (300,000 entries), and Google Cloud Audit logs (200,000 entries) provide insights into access patterns and resource activities across cloud services. Network Intrusion Detection System (NIDS) datasets, including NSL-KDD, UNSW-NB15, KDD Cup 1999, CERT Insider Threat Dataset, and the Numenta Anomaly Benchmark (NAB), were also utilized. These datasets offer a variety of network intrusion records and labelled anomalies across multiple domains, enhancing the model's ability to detect anomalies across different scenarios.

The AWS CloudTrail logs capture a comprehensive record of events within an AWS account, including both management console access and interactions via AWS CLI and APIs. This dataset helps detect anomalies in resource access and configuration changes, essential for maintaining security in AWS. Similarly, Microsoft Azure Activity Logs, accessible through the Azure portal and APIs, monitor user actions and resource operations within an Azure subscription, enabling anomaly detection and security incident analysis across various Azure environments.

In Google Cloud, Audit Logs obtained through the Google Cloud Console and APIs provide visibility into resource access and modification activities within Google Cloud Platform projects, facilitating the detection of suspicious patterns and aiding in security investigations.

Additionally, network intrusion detection datasets, such as DARPA's NSL-KDD and UNSW-NB15, are widely used benchmarks for identifying malicious traffic in network environments. NSL-KDD contains around 4 million records, while UNSW-NB15 offers a dataset of 2.5 million records, both encompassing various types of attack and benign traffic. Another benchmark, the KDD Cup 1999 dataset, contains approximately 5 million records and includes diverse attack types like Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing, making it a key resource for intrusion detection research and model development.

The CERT Insider Threat Dataset is a specialized dataset designed to simulate and study insider threat scenarios within an organizational context. It includes a diverse set of log data sources, such as host-based logs, user authentication records, and email logs, creating a comprehensive view of user activities. This dataset captures patterns and anomalies linked to insider attacks, offering valuable insights into behaviors that may signal potential security risks or unauthorized activities. By encompassing various aspects of user interactions, the CERT Insider Threat Dataset aids in developing tools and techniques for detecting and mitigating insider threats effectively.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

Table1: Average precision for identification of cloud attacks.

NT	P(%) RSSI[8]	P(%) GTM[18]	P(%) APG[41]	P(%) This Work
65k	73.21	62.05	84.41	93.42
130k	70.79	61.43	81.20	90.30
200k	70.00	63.44	84.50	98.06
265k	73.48	67.40	80.90	98.33
330k	73.59	64.44	84.80	94.31
400k	76.99	60.97	83.77	88.88
465k	71.31	63.65	87.85	96.71
530k	70.48	63.23	85.66	90.40
600k	69.34	62.73	83.77	91.43
650k	71.46	63.13	85.50	96.26
750k	74.64	63.53	83.03	95.58
800k	70.64	68.18	88.55	95.35
865k	71.65	68.41	86.23	91.63
930k	75.71	64.66	84.26	89.21
1M	72.95	63.34	87.69	93.75

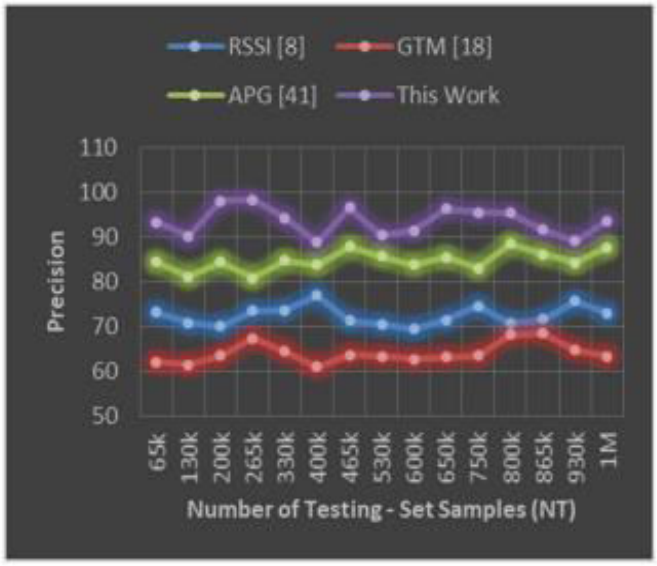

Figure1.1: Average precision for identification of cloud attacks.

Table2: Average accuracy for identification of cloud attacks.

NT	**A(%) RSSI[8]**	**A(%) GTM[18]**	**A(%) APG[41]**	**A(%) This Work**
65k	79.82	74.38	85.94	95.67
130k	80.51	72.78	86.51	89.52
200k	82.00	72.15	84.01	92.83
265k	82.63	73.21	91.89	93.27
330k	88.81	71.39	89.01	92.12
400k	85.69	76.07	90.88	97.49
465k	79.18	72.26	91.71	97.71
530k	80.87	70.04	86.35	99.50
600k	82.29	78.44	88.80	88.07
650k	86.43	71.69	91.72	92.69
750k	81.13	71.09	86.06	95.39
800k	83.20	69.54	85.91	93.81
865k	82.91	69.95	88.43	94.86
930k	80.90	73.82	89.61	92.26
1M	85.74	71.74	85.49	93.50

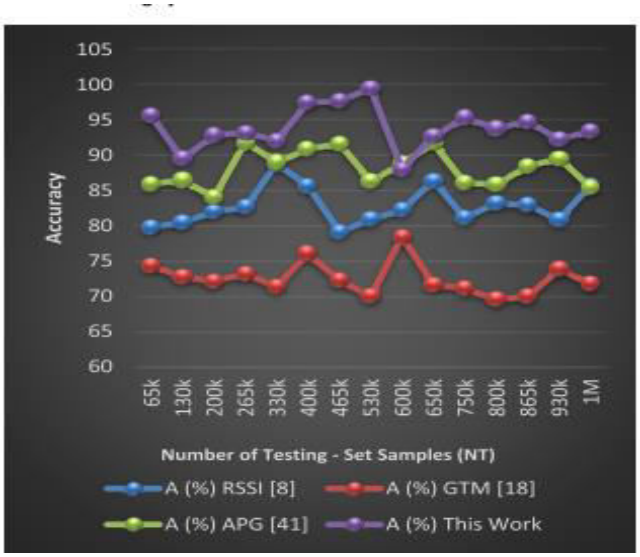

Figure2.1:Average accuracy for identification of cloud attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

Table 3. Average recall for identification of cloud attacks.

NT	R(%) RSSI[8]	R(%) GTM[18]	R(%) APG[41]	R(%) This Work
65k	79.48	75.89	83.42	91.70
130k	82.00	75.25	92.21	98.50
200k	86.98	71.99	84.72	97.72
265k	83.65	70.73	85.21	96.03
330k	79.69	70.83	85.81	98.42
400k	87.14	78.61	83.80	93.15
465k	84.45	75.41	85.70	93.58
530k	87.18	76.92	89.18	97.58
600k	82.30	73.30	86.91	94.69
650k	79.00	68.77	87.37	96.53
750k	83.70	72.79	86.19	94.65
800k	79.25	74.42	85.43	94.09
865k	81.19	75.35	87.23	92.26
930k	81.18	71.56	86.65	91.18
1M	83.07	75.24	86.16	96.38

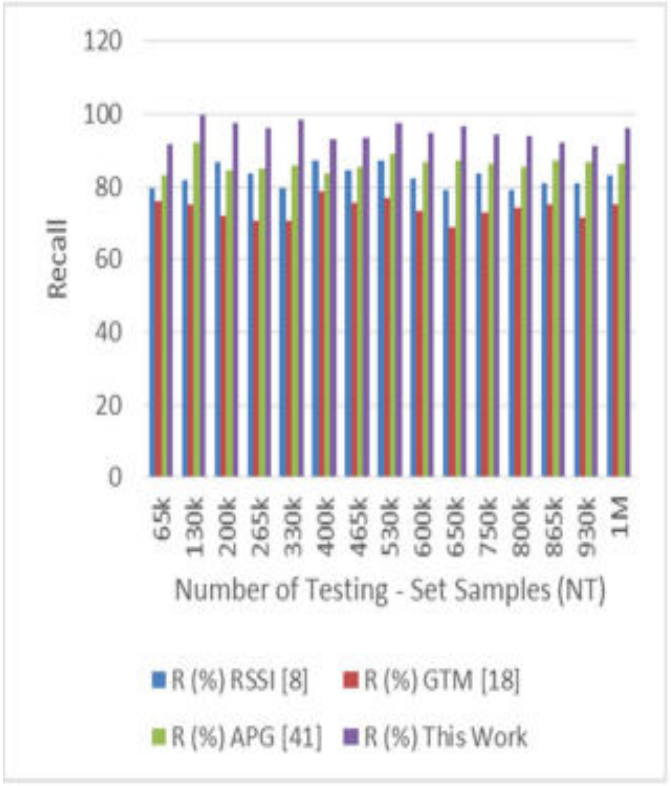

Figure 3.1 Average recall for identification of cloud attacks

V. CONCLUSION

This study uses blockchain technology to provide a novel method for cloud attack prediction and improved cloud installation performance. The suggested approach maximizes feature variability across samples by utilizing multiple deep learning models and multimodal feature analysis. According to experimental results, the model performs much better than traditional approaches (RSSI, GTM, APG) in terms of precision, accuracy, recall, and AUC. increases in precision are 3.5%, 8.5%, and 10.4%, while increases in AUC, recall, and accuracy are 12.4%, 10.5%, and 9.0%, respectively. Throughput performance, energy efficiency, and block mining delay are also assessed in the study; the suggested model outperforms RSSI, GTM, and APG in terms of speed and efficiency These results demonstrate how well the model predicts cloud threats and enhances the functionality of blockchain-based cloud installations.

REFERENCES

[1] J. Zhao, H. Huang, C. Gu, Z. Hua, and X. Zhang, ‘‘Blockchain-assisted conditional anonymity privacy-preserving public auditing scheme with reward mechanism,’’ IEEE Syst. J., vol. 16, no. 3, pp. 4477–4488, Sep. 2022.
[2] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, ‘‘Blockchain-assisted publickey encryption with keyword search against keyword guessing attacks for cloud storage,’’ IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1335–1348, Oct. 2021

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310077|

[3] H. Ghayvat, S. Pandya, P. Bhattacharya, M. Zuhair, M. Rashid, S. Hakak, and K. Dev, ''CP-BDHCA: Blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications,'' IEEE J. Biomed. Health Informat., vol. 26, no. 5, pp. 1937–1948, May 2022.
[4] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, ''A privacy-aware PUFsbased multiserver authentication protocol in cloud-edge IoT systems using blockchain,'' IEEE Internet Things J., vol. 8, no. 18, pp. 13958–13974, Sep. 2021.
[5] J. Zhang and F. Zhang, ''Identity-based key agreement for blockchain powered intelligent edge,'' IEEE Internet Things J., vol. 9, no. 9, pp. 6688–6702, May 2022.
[6] S. Itoo, A. A. Khan, V. Kumar, A. Al-Hayat, M. Ahmad, and J. Srinivas, ''CKMIB: Construction of key agreement protocol for cloud medical infrastructure using blockchain,'' IEEE Access, vol. 10, pp. 67787–67801, 2022
[7] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, ''An integrated architecture for maintaining security in cloud computing based on blockchain,'' IEEE Access, vol. 9, pp. 69513–69526, 2021.
[8] S. Benadla, O. R. Merad-Boudia, S. M. Senouci, and M. Lehsaini, ''Detecting Sybil attacks in vehicular fog networks using RSSI and blockchain,'' IEEE Trans. Netw. Service Manage., vol. 19, no. 4, pp. 3919–3935, Dec. 2022.
[9] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, ''Blockchain-envisioned provably secure multivariate identity based multi-signature scheme for Internet of Vehicles environment,'' IEEE Trans. Veh. Technol., vol. 71, no. 9, pp. 9853–9867, Sep. 2022.
[10] J. Yu, S. Liu, M. Xu, H. Guo, F. Zhong, and W. Cheng, ''An efficient revocable and searchable MA-ABE scheme with blockchain assistance for C-IoT,'' IEEE Internet Things J., vol. 10, no. 3, pp. 2754–2766, Feb. 2023.
[11] G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das, and Y. Park, ''An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment,'' IEEE Access, vol. 11, pp. 26877–26892, 2023.
[12] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, ''Post-quantum blockchain-based secure service orchestration in multi-cloud networks,'' IEEE Access, vol. 10, pp. 129520–129530, 2022.
[13] Y. Ming, C. Wang, H. Liu, Y. Zhao, J. Feng, N. Zhang, and W. Shi, ''Blockchain-enabled efficient dynamic cross-domain deduplication in edge computing,'' IEEE Internet Things J., vol. 9, no. 17, pp. 15639–15656, Sep. 2022.
[14] A. Padma and M. Ramaiah, ''GLSBIoT: GWO-based enhancement for lightweight scalable blockchain for IoT with trust based consensus,'' Future Gener. Comput. Syst., vol. 159, pp. 64–76, Oct. 2024.
[15] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, ''On cyber risk management of blockchain networks: A game theoretic approach,'' IEEE Trans. Services Comput., vol. 14, no. 5, pp. 1492–1504.
[16] M. G. Brahmam and R. V. Anand, ''MBRSDTC: Design of a multimodal bioinspired model to improve resource scheduling efficiency with differential task-level constraints,'' Expert Syst., vol. 40, no. 2, 2023, Art. no. e13302.
[17] P. Lang, D. Tian, X. Duan, J. Zhou, Z. Sheng, and V. C. Leung, ''Blockchain-based cooperative computation offloading and secure handover in vehicular edge computing networks,'' IEEE Trans. Intel. Vehicles, vol. 8, no. 7, pp. 3839–3853, Jul. 2023.
[18] C. Lin, D. He, X. Huang, and K. R. Choo, ''OBFP: Optimized blockchain-based fair payment for outsourcing computations in cloud computing,'' IEEE Trans. Inf. Forensics Security, vol. 16, pp. 3241–3253, 2021.
[19] M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi, ''A review of security vulnerabilities in Industry 4.0 application and the possible solutions using blockchain,'' in Cyber Security Applications for Industry 4.0. London, U.K.: Chapman & Hall, 2023, pp. 63–95.
[20] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, ''Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach,'' IEEE Trans. Netw. Sci. Eng., vol. 9, no. 1, pp. 271–281, Jan. 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details