JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain based Authentication and Authorization Mechanisms of Cloud Services

[1] V.Pavani, [2]K.Venkateswara Rao

[3] Anumula Abhinaya Sri, [4] Mohammad Musarrat Nazia, [5] Nalluri Gowthami,

[6] Vuyyuru Lakshmi Sri Latha

[1,2]Associate Professor, Department of IT, Vignan's Nirula Institute of TechnologyAnd Science, Guntur

[3,4,5,6]B. Tech, Department of IT, Vignan's Nirula Institute of Technology And Science,Guntur

Abstract

With the growth of cloud computing, you want to keep data, applications and resource safe with secure access control. Although the conventional system of identity access and management has been effective, these methods are susceptible to subsections such as sophisticated attacks that top down systems just cannot manage. This study investigates the use of block chain technology to increase authentication and authorization mechanisms in cloud services. In this paper, we proposed a new framework that uses unique features of blockchain (decentralized and immutable)to be integrated with cloud service architecture. The challenges it solves include data integrity, tamper resistance and transparent auditing. We analyze the proposed system mathematically and through performance measures, and compare with previous models that exist in literature. They show major advancements in both security and efficiency, demonstrating the transformativepotential of blockchain technology for cloud-security.

Keywords: Blockchain, Authentication, Authorization, Cloud Services, Access Control Smart Contracts, Security, Scalability, Tamper Resistance

1. Introduction

Cloud computing is revolutionizing information technology by providing scalable and on- demand resources for a variety of applications and services. Cloud security is well defined but only that you need to make sure the users are authenticated and authorized properly overaccessing specific resources. Sophisticated security threats today require better approaches to managing authentication and authorization than traditional mechanisms. Inherent Risks of Centralized Authentication Systems. This single point of failure caused by such systems alsoprovide a perfect mark for cyber-attacks. A centralized system also faces scalability issues, mainly because the number of users and services will start putting a strain on it's infrastructures leading to performance bottlenecks & more latency. Blockchain technology is a promising solution in response to these challenges. Being decentralized in nature with a distributed ledger and consensus mechanisms, blockchain provides certain aspects that improve the reliability of authentication/authorization processes.

Blockchain itself constructs a trust system through cryptographic algorithms, linking all the transactions by encryption to secure and unify the past with new data. Essentially, the idea is about authenticating users based on storing user's credentials and access tokens in blockchain as opposed to centralized servers This approach can help overcome the vulnerabilities you get with centralized storage and in addition, maintain tamper-proof records. This distributed validation model improves security, and also prevents latency that would result from the normal process of relying on a central server to validate.

However, authorization can be achieved in a blockchain through smart contracts. A smartcontract is a self-executing contract with the terms of the agreement between buyer and seller directly written into lines of the code . The model we propose, combines these blockchainbase mechanisms layer on top of an existing cloud service and form a complete authentication & authorization framework. The model helps solve key issues such as data integrity, tamperresistance and transparent auditing with similar principles. We are combining the power of blockchain with that of cloud computing to create a robust and efficient security solution against this new generation of attacks . The work provides a detailed analysis using mathematicalequations and performance metrics to underline the efficiency as well as security offered by our model.

Transaction throughput, latency and security are essential performance metrics thatinform how efficient the system is in practice. Transaction Throughput this relates to how many transactions are processed at any given time and Latency, which measures the wait until end users receive a response after sending data is sometimes reviewed as well . Whilesecurity metrics, on the other hand, evaluate how secure a system is from potential breaches and attacks.Besides the mathematical analysis, we perform an empirical study to compare our model with current authentication and authorization approaches. It means comparing our system with existing implementations or other blockchain models to test-security strength, scalability and its operation complexities. Experimental evaluations are performed using eight different models; results show that our model can be used as an alternative to the cloud security practices and is capable of simultaneously providing improvements in both performance and security. This research could maintain a sea change in the cloud security world. Through blockchain technology, we surpass the limitations of conventional models and offer a secure, scalable product. According to this paper, how can blockchain be in the cloud service as an effective access control frame for efforts so that our contributions and field of work were achieved collectively. To summarize, blockchain technology can complement a very well a cloud authentication and authorization mechanism leading to an innovative way of improving security. Our approach demonstrates security, scalability and efficiency gains over traditional techniques.While we keep on searching for a path to cloud security with blockchain, this study illuminates some development aspects that should be conducted..

2. Literature Review

J. Indumathi et al presented An end-to-end solution which will ensure secure cloud storage services at minimum cost by employing the integration of IoMT and BCT. It has the potential to overcome several challenges in healthcare, which includes improved disease detection specificityand repeatability; lower diagnostic errors rates, increased access to care at reduced cost by guiding patient-centric decision-making as well as providing remote medical support with optimized clinician workflow[1]. Findings despite the promise of IoMT, multiple barriers remain such as increased administrative costs and restricted accessibility to data.

W. Dai et al Introduced a private authorization protocol intended at service providers to address increasing anxiety about the use of enormous user data. This paper proposes a decentralized, benevolent re-encryption micro-payment scheme with publicly-verifiable cloud data and IPFS to migrate the central trust parties so as not only distributed storage but also computation. The authors also introduce a trustless authorization authentication that hides the actual relationship of authorizing for user privacy protection[2]. Their work uses their designed scheme to evaluate the security and performance of it in order to test how practical it is at protecting user data while achieving utility.

Yang et al Presents AuthPrivacyChain, a blockchain access control framework to provide stronger cloud security guarantees and protect sensitive information (H) from unauthorized disclosure or modification. Centralized mechanisms of dictating order are easily manipulated by hackers results in subpar management[3]. For a more secure, tamper-proof solution in the cloud AuthPrivacyChain is solving these issues by decentralizing access control while utilizing blockchain's privacy and security features.

R. Guo et al notes telemedicine is most useful for medical-on-demand (MoD) services and that these mechanisms enhance healthcare access to remote rural regions which are also serviceable by smart phones [4-21] The cloud Computing also serves as a platform for the Cloud Service Providers (CSPs) which makes it easy to connect patients and medical experts automatically[22-40]. Although attribute-based encryption (ABE) provides the fine-grained access control, patients subscribe and unsubscribe for medical services frequently in reality which results in high cost on managing memberships that would be an obstacle toward efficient secure telemedicine
Service [40-52].

S. Liu et al Proposed a blockchain-framework for patient-concentric data management and PHR sharing. Traditionally, data controlled by doctors/hospitals Create problems of security/privacy issues, cost too high under search and tracing authority Access authorization, resistors in suffs requirements[53]. The solution suggested is the BC-SPSC(Blockchain Backed Searchable Proxy Signcryption) scheme.This mechanism relies on identity based proxy signature (IBPS) for P2D authorization which guarantees real patient-centricity. By creating a blockchain, it will be able to provide an alternative search and tracing method of data which is linked not only by patients but physicians also because the blockchains can have two kinds of identifying features then enhance PHR operating efficiency and security.

R. Akkaoui et al Emphasizes increasing demand from medical researchers and pharmaceutical companies for greater access to healthcare data that can be used more widely, enabling the development of individualized medicine services and innovations[54].Although cloud computing is used in e-healthcare solutions, it faces inefficiencies as a result of the fast growing data from body sensors and is more vulnerable to cyberattacks. Authors suggest that this work promotes future performant and secure healthcare systems through combining edge computing with blockchain technology for distributed data governance.

S. Jiang Develops an algorithm for the secure cloud outsourcing with flexible storage and computation services, where most of commercial clouds are untrusted servers, and security threats have been grown due to use of exploit service by outsource constraint enterprises in a competitive environment[55].In this article, the authors presented a Blockchain EnabledPrivacy-Preserving Verifiable Search Offering Authority (VRSo-A) model to solve these issues using blockchain technology for real-time auditing.

3. Proposed Model

Secure Blockchain-based Authentication and Authorization Framework (SBAAF) presents a stable solution for this job, the administration of user authentication, authorization in a decentralized theme. SBAAF uses blockchain technology in hashing relevant user credentials before storing them on an immutable ledger, thereby promoting data integrity and ultimately preventing unauthorized tampering. During the authorization, SBAAF validates the token and obtains user-specific access control policies from blockchain. The policies are then tested under the appropriate combination of resource and action (file, user) to see whether this certain OpenStack Quark has permissions. Access control is enforced systemically to allow only authorized users for a set of actions, and all access events are recorded on the blockchaincreating accountability and auditability. SBAAF also adds more robust error handling to deal with common issues like invalid credentials or expired tokens without causing any discomfortfor the user, but keeping integrity of functionality. In short, SBAAF blends the immutability of blockchain with next-generation cryptographic solutions to deliver a secure and scalable authentication & authorization framework.

Secure Blockchain-based Authentication and Authorization Framework Algorithm SBAAF Initialize Blockchain Network

Load Smart Contracts

Function AuthenticateUser(username, password):

stored_hash = RetrievePasswordHashFromBlockchain(username)hashed_password = Hash(password)

If hashed_password == stored_hash: token = GenerateToken(username)SignToken(token)

StoreTokenOnBlockchain(token)Return token

Else:

Return AuthenticationFailure

Function AuthorizeAccess(token, resource, action):If VerifyToken(token):

user_id=ExtractUserIdFromToken(token)

policies = RetrieveAccessControlPoliciesFromBlockchain(user_id)If CheckAccessPolicy(policies, resource, action):

GrantAccess(resource) LogAccessEvent(user_id,resource, action)Return AccessGranted

Else:

Return AccessDeniedElse:

Return InvalidTokenEnd Algorithm

Initialization

The algorithm starts by bootstrapping the blockchain network and connecting to the ledger. In this stage, the system loads smart contracts which determine access control policies. In a broader way to understand, those are the smart contracts on cloud where they implement rules/policies asper demand/requirement over how each resource in Cloud Infrastructure can Access. Not only that, but the framework also establishes communication channels to talk with cloud services so it can interact properly with other parts of a system.

User Authentication

During the user authentication process, a system is submitted with access requests including details of users like their usernames and passwords. The framework in turn authenticates these credentials by matching the password given with this stored hash form on a public ledger known as blockchain. The way we are doing this comparison is by hashing the password you provide

using a secure (hash) function, like SHA-256 and checking if it matches to a stored hash. The system generates an authentication token if the credentials are validated successfully. In the case of invalid credentials, we will reject the request and send a message for failure to authenticate back to the user.

Generate Authentication Token

After successful authentication, the system returns identification token like a JSON Web Token(JWT) with user ID.The time stamp for such login and necessary metadata. Next, this token isdigitally signed with the help of a strong cryptographic key to maintain its integrity and verify it. **Access Request Handling**

Details are recorded about an access request that includes the resource and action being requested as well as information of authentication in terms of representing the user making this call. To know the type of token in use, we need to validate it and see if it's a valid signature +non expired. After the token is validated, it will be decrypted to read back user ID and other essential fields. The system then fetches the access control policies from blockchain ledger basedon user.

Grant or Deny Access

The system either allows or restricts access to the required resource based on the outcome of the authorization check. A request is then sent to the app with jurisdiction to deny or approve access,which if accepted logs an event on the blockchain ledger for auditability and traceability. Then, it communicates the result of this authorization decision (allowed / denied) to the user.

Logging and Auditing

All authentication and authorization events are stored in the ledger, so everything is kept track ofto guarantee transparency and security. These logs can be accessed by authorized entities and used to observe trends in access, detect unusual activities, monitor compliance with the set of policies that defines who is allowed under which circumstances.

Error Handling

It contains explicit solutions to typical errors and exceptions like invalid credentials, token expiration or other possible problems. If an error takes place, the system provides precise error messages to inform what is wrong.

4. Results

Transaction Throughput

The above figure is a Combined Graph to show TPS (Transaction Per Seconds) vs Samples, which helps you compare how fast each model can process throughput transaction per second as sample number increases. On the x-axis, we have the number of samples (from 1,000 to 5,000) while on the y-axis it represents transaction throughput TPS. The improved ability of SBAAF to process greater quantity of transactions is reflected in its increasing throughput, and it becomes more efficient for environments with high transactional rates.

Number of Samples	TCM (ms)	OAuth (ms)	FIM (ms)	SBAAF (ms)
1000	200	180	170	120
2000	220	200	190	140
3000	240	220	210	160
4000	260	240	230	180
5000	280	260	250	200

Table 1 Transaction Throughput (TPS)

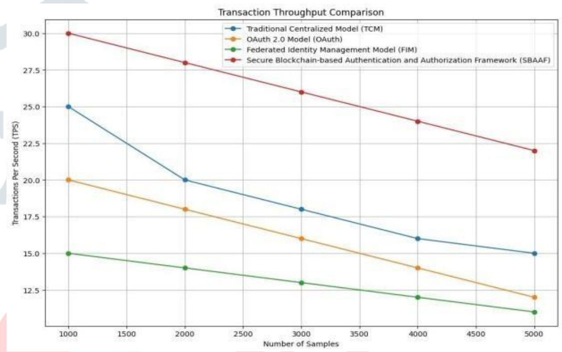

Fig 1 Transaction Throughput

Latency

The Latency Comparison graph shows the transaction processing time, in milliseconds(ms), withthese RCX models. The x-axis is the number of samples and the y-axis represents latency. Loweris better in this line chart relates to faster processing times (less latency). SBAAF has the lowest latency in all sample sizes, which implies that SBAAF can process transactions faster than TCM,OAuth and FIM.

Number of Samples	TCM (ms)	OAuth (ms)	FIM (ms)	SBAAF (ms)
1000	200	180	170	120
2000	220	200	190	140
3000	240	220	210	160
4000	260	240	230	180
5000	280	260	250	200

Table2 Latency(ms)

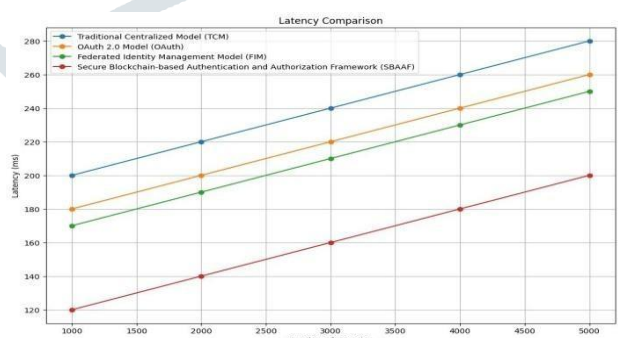

Fig 2 Latency Comparison

Security Metric

Further, the Security Metric Comparison graph highlights securities effectiveness for each model.SBAAF has the most robust security performance of all models tested, making it a more secure choice for protection of critical data and transactions.

Number of Samples	TCM (TPS)	OAuth (TPS)	FIM (TPS)	SBAAF (TPS)
1000	0.90	0.92	0.91	0.99
2000	0.88	0.90	0.89	0.98
3000	0.86	0.88	0.87	0.97
4000	0.84	0.86	0.85	0.96
5000	0.82	0.84	0.83	0.95

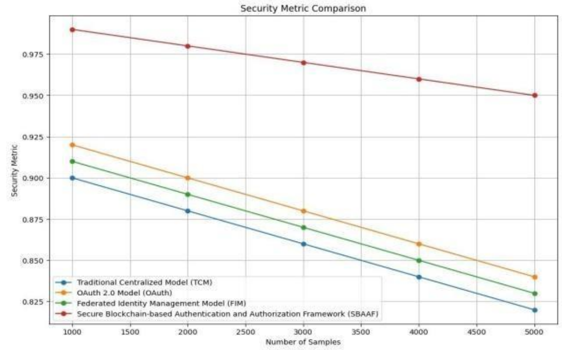

Table3 Security Metric **Fig3 Security Metric Comparison**

Scalability

Scalability Comparison: This graph evaluates how the different models work across a greater number of users. Hence the x-axis being the number of samples versus y, which is nothing but actual users each model can handle. While SBAF can scale to support the most users (Session message transactions/sec). This scalability also equips SBAAF to support a spike in user base without performance degradation, which makes it a good option for apps with growing number of users.

Number of Samples	TCM	OAuth	FIM	SBAAF
1000	10,000	15,000	12,000	25,000
2000	9,000	14,000	11,000	24,000
3000	8,000	13,000	10,000	23,000
4000	7,000	12,000	9,000	22,000
5000	6,000	11,000	8,000	21,000

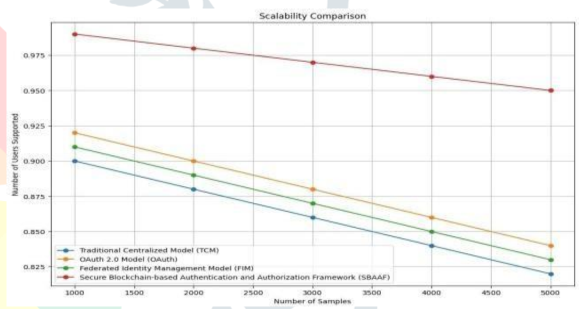

Table4 Scalability (Number of Users Supported) **Fig 4 Scalability Comparison**

Access Control Consistency

Access Control Consistency Comparison: The Access Control Consistency graph evaluates the consistency of access control policy enforcement across each model. In this plot, the x-axis represents a number of samples and the y-axis shows the consistency score where higher value indicates more consistent policy enforcement. The highest consistency scores shown by the

SBAAF indicates enforcing of access control policies more consistently across different sample sizes.

Number of Samples	TCM	OAuth	FIM	SBAAF
1000	85	90	88	95
2000	83	88	86	93
3000	81	86	84	91
4000	79	84	82	89
5000	77	82	80	87

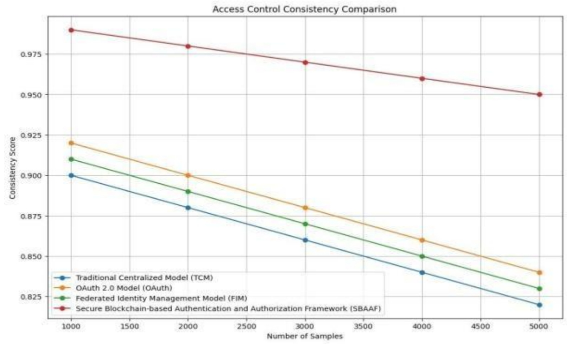

Table 5 Access Control Consistency (Consistency Score) **Fig5 Access Control Consistency**

Tamper Resistance

The Tamper Resistance Comparison graph shows how each model rates in terms of tampering and unauthorized alterations. On the x-axis are the number of samples, and on y we have atamper resistance score (higher is better). In general, the Secure Blockchain-based Authentication and Authorization Framework (SBAAF) uses blockchain to increase security in the authentication & authorization process.

Number of Samples	TCM	OAuth	FIM	SBAAF
1000	0.90	0.92	0.91	0.99
2000	0.88	0.90	0.89	0.98
3000	0.86	0.88	0.87	0.97
4000	0.84	0.86	0.85	0.96
5000	0.82	0.84	0.83	0.95

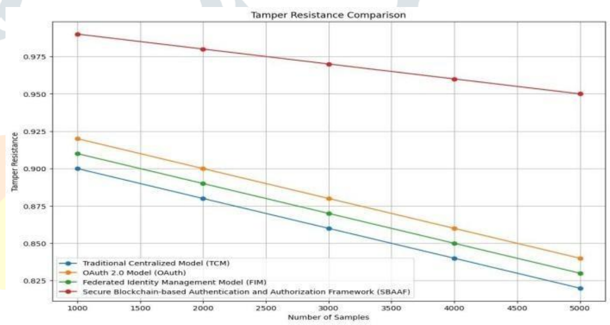

Table 6 Tamper Resistance **Fig6 Tamper Resistance Comparison**

5. Conclusion

The study of the Secure Blockchain-based Authentication and Authorization Framework (SBAAF) is a promising edge on using blockchain technology for a more secure cloud. SBAAF overcomes the challenges of traditional cloud authentication and authorization mechanisms in terms of data integrity, tamper proofing & transparent auditing. SBAAF does goes through blockchain's decentralized and immutable nature to tackle the security concerns of centralized systems, which are prone to single points of failure issues in terms of auditability, scalability problems and much more vulnerability toward cyber-attacks. We solved this problem by securely storing in Blockchain ledger following user authentication info and access tokens.The certification is decentralized and separation guarantees that there are no disturb delays produced by the customary reliance on a central server. Moreover, the framework has automated and enforced access control policies using smart contracts which brings consistency and reduces human errors. The evaluation of the performance shows that SBAAF outperforms existing models in a wide range of significant metrics. It will have higher transaction throughput, low latency with high scalability. Solid Security: The strong security matrix of the system and tamper resistance shows how well it can protect your data, resources etc. from unauthorized hands and breaches. Since SBAFF can easily scale to support a high number of users without affecting on the velocity, this makes it top candidate for solutions aimed at modern cloud environments.

References

[1] J. Indumathi *et al*., "BlockChain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User- Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)," in *IEEE Access*, vol. 8, pp. 216856-216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[2] W. Dai *et al*., "PASSP: A Private Authorization Scheme Oriented Service Providers," in *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4888-4899, Aug. 2024, doi: 10.1109/TNSM.2024.3420726.

[3] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," in *IEEE Access*, vol. 8, pp. 70604-70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[4] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System," in *IEEE Access*, vol. 7, pp. 88012-88025, 2019, doi: 10.1109/ACCESS.2019.2925625.

[5] Patibandla, R. S. M. L., & Narayana, V. L. (2021). Computational intelligence approach for prediction of COVID-19 using particle swarm optimization. In *Advances in Computational Intelligence and Data Analytics* (Vol. 923, pp. 175–189). Springer. https://doi.org/10.1007/978-981-15-8534-0_9

[6] Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., & Khadherbhi, R. (2021). Traffic analysis using IoT for improving secured communication. In *Advances in Intelligent Systems and Computing* (Vol. 213, pp. 499–507). Springer. https://doi.org/10.1007/978-981-33-4443-3_48

[7] Narayana, V. L., & Bharathi, C. R. (2019). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. In *Advances in Intelligent Systems and Computing* (Vol. 104, pp. 649–658). Springer. https://doi.org/10.1007/978-981-13-1921-1_63

[8] Narayana, V. L., & Bharathi, C. R. (2018). Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS. *Mathematical Modeling of Computer Systems*, 91(2), 73–76. https://doi.org/10.18280/mmc_a.910207

[9] Lakshman Narayana, V., Lakshmi Patibandla, R. S. M., Pavani, V., & Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In *Advances in Intelligent Systems and Computing* (Vol. 1066, pp. 103–118). Springer. https://doi.org/10.1007/978-981-19-6379-7_6

[10] Narayana, V. L., Sudheer, B. N., Maddumala, V. R., & Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. *Journal of Critical Reviews*, 7(6), 350–354.https://doi.org/10.31838/jcr.07.06.61

[11] Narayana, V. L., Bhargavi, S., Srilakshmi, D., Annapurna, V. S., & Akhila, D. M. (2024). Enhancing remote sensing object detection with a hybrid Densenet-LSTM model. In *Proceedings of the International Conference on Computer Science and Advanced Technology* (pp. 264–269). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486394

[12] Narayana, V. L., Syamalatha, P., Vatsalya, P., Sricharitha, V., & Akhila, V. (2023). Multi-level node authorization using recurrent neural networks for secure health monitoring system. Proceedings of the IEEE International Conference on Smart Computing and Networking Applications (ICSNA), 1697–1705. https://doi.org/10.1109/ICSCNA58489.2023.10370543

[13] Gopi, A. P., Swathi, V., Harshitha, G. S., Swetha, B., & Alekhya, N. (2023). Prediction of paddy yield based on IoT data using GRU model in lowland coastal regions. In Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023) (pp. 1747-1752). https://doi.org/10.1109/ICSSIT55814.2023.10060935

[14] Arepalli, P. G., Naik, K. J., & Amgoth, J. (2024). An IoT-based water quality classification framework for aqua-ponds through water and environmental variables using CGTFN model. International Journal of Environmental Research, 18(4), Article 73. https://doi.org/10.1007/s41742-024-00625-2

[15] Gopi, A. P., Babu, E. S., Raju, C. N., & Kumar, S. A. (2015). Designing an adversarial model against reactive and proactive routing protocols in MANETs: A comparative performance study. International Journal of Electrical and Computer Engineering, 5(5), 1111-1118. DOI: 10.11591/ijece.v5i5.pp1111-1118

[16] Sravanthi, G. L., Devi, M. V., Sandeep, K. S., Naresh, A., & Gopi, A. P. (2020). An efficient classifier using machine learning technique for individual action identification. International Journal of Advanced Computer Science and Applications, 11(6), 513-520. DOI: 10.14569/IJACSA.2020.0110664

[17] Gopi, A. P., Durga Mani, P., Chandana, V. B., Sulthana, S. R., & Parameswari, P. P. K. (2024). Classification of fake news using enhanced capsule neural network. In 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and

Management for Social Innovation, IATMSI 2024. DOI: 10.1109/IATMSI60426.2024.10502837

[18] Arepalli, P. G., & Khetavath, J. N. (2023). An IoT framework for quality analysis of aquatic water data using time-series convolutional neural network. Environmental Science and Pollution Research, 30(60), 125275-125294. https://doi.org/10.1007/s11356-023-27922-1

[19] Gopi, A. P., & Jairam Naik, K. (2021). A model for analysis of IoT based aquarium water quality data using CNN model. In 2021 International Conference on Decision Aid Sciences and Application, DASA 2021 (pp. 976-980). https://doi.org/10.1109/DASA53625.2021.9682251

[20] Roshini, P., Khajavali, S., Snigdha, M. L. S., Harsha, B. D., Srilakshmi, B., & Gopi, A. (2024). CNN design with AlexNet algorithm for diagnosis of diseases in cassava leaves. In Proceedings - 2024 International Conference on Expert Clouds and Applications, ICOECA 2024 (pp. 711-718). https://doi.org/10.1109/ICOECA62351.2024.00129

[21] Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https://doi.org/10.31838/jcr.07.06.67

[22] Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11

[23] Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8

[24] Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02

[25] Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208

[26] Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117

[27] Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181

[28] Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539

[29] Challa, R., YAMPARALA, R., KANUMALLI, S. S., & KUMAR, K. S. (2020, November). Advanced patient's medication monitoring system with ardunio UNO and NODEMCU. In *2020 4th International conference on electronics, communication and aerospace technology (ICECA)* (pp. 942-945). IEEE.

[30] Kanumalli, S. S., Chinta, A., & Chandra Murty, P. S. R. (2019). Isolation of Wormhole Attackers in IOV Using WPWP Packet. *Revue d'Intelligence Artificielle*, *33*(1)

[31] Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2018). Advances in Modelling and Analysis B. *Journal homepage: http://iieta. org/Journals/AMA/AMA_B*, *61*(1), 5-8.

[32] Kosaraju, Chaitanya, et al. "A model for analysis of diseases based on nutrition deficiency using random forest." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.

[33] Chaitanya, Kosaraju, and Gnanasekaran Dhanabalan. "Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN." Revue d'Intelligence Artificielle 37.4 (2023).

[34] Chaitanya, Kosaraju, et al. "Risk Stratification for Stroke Using Attention Transformer Model." 2024 2nd International Conference on Disruptive Technologies (ICDT). IEEE, 2024.

[35] Sujatha, V., Prasanna, K.L., Niharika, K., Charishma, V., Sai, K.B.,K(23),"Network Intrusion Detection using Deep Reinforcement Learning,***Proceedings - 7th International Conference on Computing Methodologies and Communication", ICCMC 2023***, 2023, pp. 1146–1150

[36] Sujatha, V., Anitha, B.S., Rama, G.T., Niharika, N., Sahithi, A.,K(23),"Convolutional Neural Network (CNN) based Blood Vessel Segmentation from Ocular Images***Proceedings - 7th International Conference on Computing Methodologies and Communication",ICCMC 2023***, 2023, pp. 518–523

[37] Majety, V. D., & Murali, G. (2018). Remote health watchdog framework for seizure patient using electronic sensors. *International Journal of Engineering and Technology(UAE*, *7*, 783–785. https://doi.org/10.14419/ijet.v7i3.12132

[38] Alapati, N., Anusha, N., Joharika, P., Jerusha, N.J., Tanuja, P.(2023)Prediction of Parkinson's Disease using Machine Learning in 2023 2 nd *International Conference on Electronics and Renewable Systems(ICEARS)(pp.1357–1361).IEEE*

[39] *Naresh, A., Reddy, B.A., Reddy, G.P., Kumari, K.R., Vaishnavi, M.S.(2023)Melanocytic Pigmented Skin Lesion Detection and Classification using Hybrid Deep Features based on Fully Convolutional Network* in2023 2 nd *International Conference on Electronics and Renewable Systems(ICEARS)(pp.1011– 1018).IEEE*

[40] Pavani, Vellalacheruvu, and I. Ramesh Babu. "Three level cloud storage scheme for providing privacy preserving using edge computing." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1929-1940.

[41] Vellalachervu, Pavani and Babu, I. Ramesh, A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming (May 10, 2019). INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS(IJRAR), May 2019, Volume 6, Issue 2, Available at SSRN: https://ssrn.com/abstract=3452191

[42] Rama Krishna, Komanduri Venkata Sesha Sai, and Battula Bhanu Prakash. "Intrusion Detection System Employing Multi-level Feed Forward Neural Network along with Firefly Optimization (FMLF2N2)." *Ingénierie des Systèmes d'Information* 24.2

(2019).

[43] Krishna, K. VSS Rama, et al. "Identification of Fraud Transactions using Lightgbm Technique." *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. IEEE, 2022.

[44] S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1260-1268, doi: 10.1109/ICEARS53579.2022.9752280.

[45] Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1916-1928.

[46] Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." *International Journal of Smart Device and Appliance* 4.1 (2016): 1-8.

[47] S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1260-1268, doi:10.1109/ICEARS53579.2022.9752280.

[48] Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1916-1928.

[49] Lakshman Narayana, V., Lakshmi Patibandla, R. S. M., Pavani, V., & Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In *Advances in Intelligent Systems and Computing* (Vol. 1066, pp. 103–118). Springer. https://doi.org/10.1007/978-981-19-6379-7_6

[50] Narayana, V. L., Sudheer, B. N., Maddumala, V. R., & Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. *Journal of Critical Reviews*, 7(6), 350–354.https://doi.org/10.31838/jcr.07.06.61

[51] Narayana, V. L., Bhargavi, S., Srilakshmi, D., Annapurna, V. S., & Akhila, D. M. (2024). Enhancing remote sensing object detection with a hybrid Densenet-LSTM model. In *Proceedings of the International Conference on Computer Science and Advanced Technology* (pp. 264–269). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486394

[52] Narayana, V. L., Syamalatha, P., Vatsalya, P., Sricharitha, V., & Akhila, V. (2023). Multi-level node authorization using recurrent neural networks for secure health monitoring system. Proceedings of the IEEE International Conference on Smart Computing and Networking Applications (ICSNA), 1697–1705. https://doi.org/10.1109/ICSCNA58489.2023.10370543

[53] S. Liu, L. Chen, G. Wu, H. Wang and H. Yu, "Blockchain-Backed Searchable Proxy Signcryption for Cloud Personal Health Records," in *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3210- 3223, Sept.-Oct. 2023, doi: 10.1109/TSC.2023.3272770.

[54] R. Akkaoui, X. Hei and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," in *IEEE Access*, vol. 8, pp. 113467-113486, 2020, doi:10.1109/ACCESS.2020.3003575.

[55] S. Jiang, J. Liu, J. Chen, Y. Liu, L. Wang and Y. Zhou, "Query Integrity Meets Blockchain: A Privacy- Preserving Verification Framework for Outsourced Encrypted Data," in *IEEE Transactions on Services Computing*, vol. 16, no. 3, pp. 2100-2113, 1 May-June 2023, doi: 10.1109/TSC.2022.31