Blockchain-Based Privacy Conservation Framework

S P Maniraj[1] P. Robert[2] Ravilla Pavithra[3] and J. Omana[4]

[1]Department of Computer Science & Engineering, S.R.M. Institute of Science and Technology, Chennai, Tamil Nadu, India
[2]Department of Artificial Intelligence & Machine Learning, C.M.R. Institute of Technology, Bengaluru, Karnataka, India
[3]Department of Computer Science & Engineering, R.M.D. Engineering College, Chennai, Tamil Nadu, India
[4] Department of Information Technology, Prathyusha Engineering College, Chennai, Tamil Nadu, India
spmaniraj1986@gmail.com

Abstract. As the blockchain architectures and communities grow, blockchain networks frequently face scenarios where the user must vote to make decisions. However, a natively implemented voting system on current blockchain systems is useless. The decision-making process is then either assigned to many network members who make such decisions offline or reliant on online voting services by third parties. The peers depend on reliable parties or centralized networks directly or implicitly. This contradicts the underlying blockchain decentralization theory and opens the option to theft. The work suggests a native blockchain voting protocol for peers to vote on their existing block-chained network without requiring a responsible or third party to enable decentralized and secure decisions. The protocol protects end-to-end anonymity and has attractive properties such as cheating detectability and correctness. A protocol for the legitimacy and functional applicability of protocol on Hyperledger Fabric shall also be enforced.

Keywords: Ethereum, E-Voting, Block Chain, Hyper Ledger, Privacy, Transaction Accuracy.

1 Introduction

The awareness of blockchain technology has significantly increased since Satoshi Nakamoto released the first edition of the Bit coin white paper in 2008 [1-2]. Exposure to the capabilities of the technology reached an all-time high when it was discovered that Ethereum could function as a turing complete platform to carry out many complicated mathematical operations on a blockchain network [3]. After that, various exciting and cutting-edge apps were developed to run on the Ethereum blockchain. The Decentralized Autonomous Organizations (D.A.O.) was responsible for founding many organizations, one of which was a scattered independent association [4]. It was a venture capital fund owned by investors and ushered in a new age of corporate lead-

R. Murugan et al. (eds.), *Proceedings of the International Conference on Signal Processing and Computer Vision (SIPCOV 2023)*, Advances in Engineering Research 239,
https://doi.org/10.2991/978-94-6463-529-4_29

ers. Over the next month and a half, the D.A.O. will become the first firm to be crowd-funded, with a token sale in May 2016 raising over 150 million dollars.

However, cyber-antiques on the D.A.O. network led to the theft of ether worth $60 million immediately after fund-building [5-6]. This theft occurred right after the operation. This attack presented a problem to the Ethereum base and the Ethereum network runners (miners), namely whether the Ethereum base should accept the assault or construct a gateway to invalidate the assault and minimize the damage [7]. To provide the groundwork for Ethereum, the miners were necessary to decide whether or not they should have elections. However, the Ethereum network cannot enable this vote's situation in any way [8].

Miners either had to focus on the ad-hoc vote method of their mining pool operated by mining pool management or used a community-based vote The latter might be accomplished by transferring "Sudo ethers" to two addresses under the control of outside entities [9]. More implementations in the real world are foreseen to use Blockchain as the platform matures. This can expect that different vote events may occur in the future. Thus, a local voting system set up on the Blockchain Network is required to decentralize and disintermediate [10]. Moreover, it argues that such a voting method is not only necessary for public blockchain networks. Hyperledger Fabric [11] is only one example of a blockchain consortium-approved network that supports it. Accepted blockchains often do not allow for the concept of mining, and network runners are instead seen as peers. To minimize confusion, "peer voting" describes miners' and peers' participation in a block chain's publishing and permission processes [12]. Votes are a common phenomenon because, in one way or the other, it is a part of different cultures. Pair voting, however, varies from voting, such as presidential votes. It is typically performed digitally rather than conventional (physical) voting and thus poses multiple forms of difficulties. As summarized, there are several attractive features for an optimal online voting system [13-14]. The most important are:

Eligibility: Voting is only possible if it's been authorized. The number of voters available to miners on the public blockchain network is restricted, and voting occurs among peer members of the blockchain consortium in pairs [15]. In such circumstances, voters must already have the underlying network authorized on their devices. There is no cause for alarm about the attack on Sybil.

Integrity: It is impossible to change, counterfeit, or retract votes that have been cast undetected [16]. Auditability requires reviewing each vote to ensure that it is adequately recorded in the tally. Auditability Peer voting on a blockchain should satisfy not only these precise criteria but also the standards outlined below for voting in the real world, precisely: protection of privacy from beginning to end votes cast by voters should never be made available to anybody, at any time [17].

Detection and correction: Any dishonest count may be corrected, and an invalid or fraudulent vote found and removed from the tally. There is no need for secret approval [18]. Due to the distributed nature of a blockchain network, this is necessary. A well-designed system currently needs to be made available to perform peer voting. Many of the online voting systems that now exist need to fulfil the criteria listed above [19]. Many of these systems fail because the detection/correction is based on

trustworthy authority. No simple extensions are also possible. Later, a thorough overview of these current choices will be shared in the literature review part. A voting protocol for privacy without a responsible party supplying the desired properties for the abovementioned peer voting is suggested to fill the void. 1) Delivery votes are the main proposals. Several ballots to a peer rather than one vote per peer are delegated. Their vote mode specifies the purpose of voting for the peer. This feature guarantees that voting secrecy is maintained [20]. The voting decision will be shown only once the bulk of the votes is exposed. A vote's total cannot be revealed by its presentation alone. Using homomorphic encryption, this technique may distribute votes among participants without letting anybody see the final tally. Because of this principle, a trustworthy tally team is optional. Verification based on cryptography. Testing the votes and counting means that people's deceptive behavior is observed in the procedure. Moreover, when the check can be carried out openly without compromising data security, there is no trustworthy party required .

2 Literature Review

An online vote method in literature has been a hot topic for a long time. Over the years, several multiparty vote algorithms have been proposed to protect the confidentiality and transparency of voting information online. According to [21], a vote's anonymity may be preserved in two ways: either by encrypting the voice beforehand or by sending it over an anonymous communication channel. The first technique was suggested for encrypting the ballot. However, owing to the amount of contact required to check the votes, all these steps became rather impractical. This solution was realistic in that it needed coordination. Still, it also posed other issues, including the central authority's reliance on votes and the opportunity for a clash by using random lines to discriminate between each ballot [22]. This approach was also more practical.

It is suggested that a non-interactive secret sharing mechanism, which could be used in public authentication of votes and the defense of voters' privacy, using homomorphic encryption technologies. Once again, however, this required some higher power to step in and decipher the ballots to accord with the final tally. The user already has a receipt, which raises concerns that their vote's anonymity may be at risk if they publicize that record. Thus, different voting mechanisms free of reception have also been requested [23]. It is proposed that a mere scheme of elections containing multi-government votes in which a single vote (encrypted message) is posted with evidence that the ballot includes a legitimate vote.

Finally, also sites for online voting, e.g., HELIOS, it was also observed that online voting was made simpler by using Web technology. Although these voting platforms were not planned for high-level elections, there were significant protection and consumer privacy deficiencies, demonstrating how voting outcomes can be manipulated by current customer site vulnerabilities [24]. These electronic voting systems rely on a single point of failure, which increases their susceptibility to breaches that might undermine voter anonymity, election administration integrity, and public trust. It has shown that a fraudulent electoral official can handle an election by supplying crypto-

graphic confirmation that the votes have been counted accurately by an arbitrary outcome.

As most online voting occurs in the public domain, it suggests using a hidden mask to mask each user's vote for non-receiving online elections. This paper proposes the D- DEMOS distributed electronic voting system, which is verifiable end-to-end and preserves privacy without requiring client-side encryption processes [25]. This is made possible through a distributed voting subsystem that collects user votes and forwards them to a newsletter board, which is also distributed. The electronics authority that now proves that voting inside a voting box is lawful since D-DEMOS adopted the Chaum-Pedersen zero-knowledge proof. However, the Bulletin Board portion of this approach still requires a trustee subsystem with encryption keys to access the vulnerable material.

As most online voting occurs in the public domain, it suggests using a hidden mask to mask each user's vote for non-receiving online elections. This paper proposes the D- DEMOS distributed electronic voting system, which is verifiable end-to-end and preserves privacy without requiring client-side encryption processes [26]. This is made possible through a distributed voting subsystem that collects user votes and forwards them to a newsletter board, which is also distributed. The electronics authority that now proves that voting inside a voting box is lawful since D-DEMOS adopted the Chaum-Pedersen zero-knowledge proof. However, the Bulletin Board portion of this approach still requires a trustee subsystem with encryption keys to access the vulnerable material.

To facilitate national elections, a blockchain-based voting network has been proposed. Their solution still relied on a responsible third party to conceal a vote from an election organization. The major challenge with this strategy was that the secret vote would easily be compromised if the trusted third party got the identity id. This also suggests developing a democratic online voting mechanism to bypass the different central authorities, leveraging blockchain technologies. It also highlights that conventional online voting challenges already remain on the market for new blockchain-based voting solutions.

Until now, most of the electronic systems based on Blockchain have been designed to promote some online general elections. In activities where audience members have to make such decisions and hold a vote, it relies on current online voting systems. There is no way to allow existing network partners to vote on any new blockchain networks [27]. This paper suggests that a protocol for voting for peers on a blockchain network, which is free of reception, can be checked and preserves their privacy. For voting recognition or voting tallying, no responsible third party is needed. This protocol uses basic cryptography using public key cryptography. Homomorphic cryptography employs the consensus process intrinsic to blockchain technology to encourage peer votes on Blockchain while meeting all the conditions for a fair and secure voting event. In addition, a strategy outlined for dispersed voting and tallying is adopted while ensuring public verification to safeguard voting secrecy.

3 Proposed System

The suggested design includes four layers: layer for user interaction and front-end security, layer for access control management, layer for managing electronic voting transactions, and a layer for synchronizing the ledger. Figure 1 illustrates the proposed voting system's general architecture based on blockchains. Following is an explanation of the intricate operating mechanism that is included in each layer.

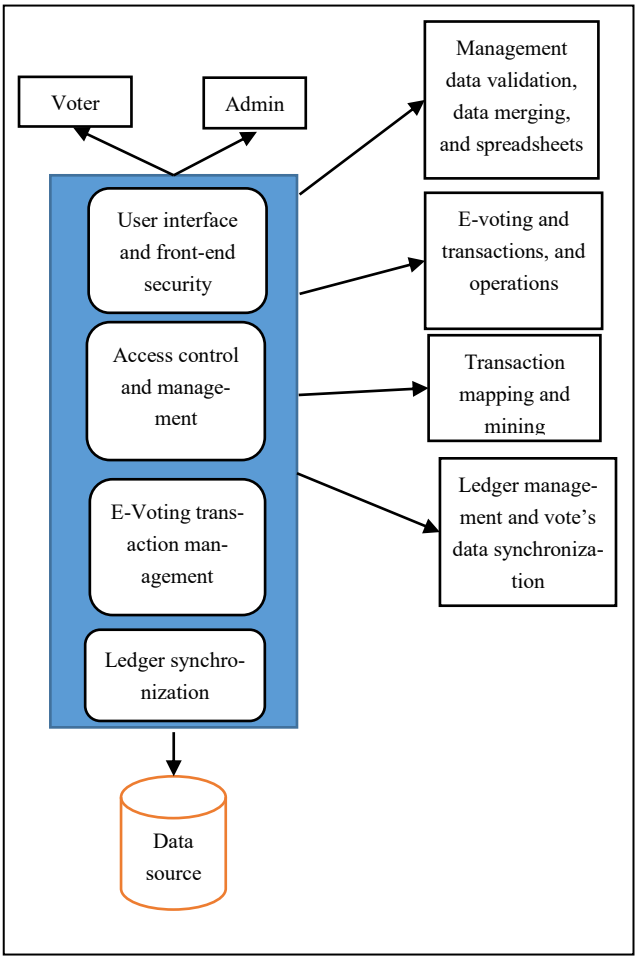

Fig. 1. Proposed block chain-based voting system.

User Interaction and Front-End Security Layer

It has a connection that is established directly with the voter. Voters and administrators may have conversations with it. The authentication and permission of users is the primary function of this layer's responsibilities. The primary duty of this layer is to

authenticate voters' credentials following the policy being implemented by the government.

Access Control Management Layer

It facilitates layers one and three by delivering the necessary services to accomplish the intended tasks. The most important duties and responsibilities are defining access control regulations and voting policies and establishing job definitions. The definition and administration of roles are the essential support needed by Layer 1. At the same time, defining transactions is the most important type of support required by Layer 3. Therefore, this layer functions as a coherent layer between the first and third layers.

E-Voting Transaction Management layer

It is the primary layer of the blockchain architecture that has been suggested. In this case, the electronic voting transactions are constructed as blockchain transactions, which must be mined. The voting data are created using cryptographic hash algorithms, and the transaction I.D.s is used to build the data. This layer oversees ensuring that mining operations successfully contribute monetarily to the Blockchain.

Ledger Synchronization layer

It is responsible for storing the multi-chain ledger in the database customized to the local area. The cryptographic hashes used for end-to-end communication security also include the voter's security concerns. These databases are used to record the outcomes of the vote to make the auditing and processing of those results easier at a later stage.

The working mechanism of the proposed framework

It shall begin by explaining in this portion, during some technical assumptions, the main concept of protocol design. We will proceed with the technical information later. Recognizing and correcting dishonest behaviors during peer voting is made more difficult by the need for anonymity without a dedicated group. It suggests two essential ideas to protocol design to address this problem. Divining into several sections and allocating to several randomly chosen peers, each vote is interpreted as a distribution. Each segment should be automatically checked, and a limited set does not indicate the general preference for the ballot. Complete voting is allocated to each pair, and a small fraction is counted for each pair. Each count of each peer can be reviewed and corrected, and all valid partial counts are applied to produce the final vote results. Before thoroughly explaining the protocol, it prepares a few remarks and observations.

Suppose that there are n peers, Pj (1), who may take part in the vote on a blockchain network2. During the election period, the cumulative number of electors would not rise. The choice selection C of an alternative in ballot B is deemed to be correct when represented by the following,

C = Ni–1 + r optional N, 1 = optional N

where r is the random number after encryption to safeguard the privacy of the preference. A homomorphic script three is used in each ballot to encrypt the option. The private key HESKj and the public key HEPKj are generated by each voter Pj. The coding of the option is used for each vote Pj. *Digital Signature* ECDSA is used. Voting Pj establishes his Signing private key Pair (SigPKj, SigSKj).

If one is a part of any of these three groups, a peer is dishonest: I Dishonest Elector, if he presents an illegitimate ballot. The reporter of Unethical if he does not announce his HEPK encrypted voting with a base choice. Fraudulent counter if the legitimate votes encoded by his HEPK have been released in inaccurate tally data. The proposed protocol consists of five steps involving off-chain consumer applications calculations and smart contracts executing online computations.

Electors (including two public keys [HEPKj, SiPKj] are reported. At this point, voters can use customer applications in the voting time window for planning and voting on Blockchain. Each transaction submitted will be authenticated on Blockchain and reported as accurate on the ledger. Each ballot is reviewed in two phases. During this point, the pair whose HEPK is used to encrypt the vote will decrypt and check each franchise. Invalid ballots to Blockchain should be registered.

Smart contracts to verify these recorded ballots can be checked (dishonest reporting). If a deceptive reporter is found, it is essential to locate and replace all the votes encrypted by HEPKj. If a revolting transaction doesn't require a new vote, move to stage 4 and replicate stage 2 to validate the new voting. Note that if a peer fails to cast replacement votes before the expiration of the revocation term, it can be considered the replacement of the peer. Due to this reduction, there may be a slight change in the result of the votes, but only if the number of votes to be replaced is much fewer than K and if there is sufficient time to withdraw them before the deadline.

Both legitimate ballots during this process are determined by peers whose rank is still allocated as "honest," that is, each pair is responsible for his share. Each tally result is blockchain-published. Intelligent contracts will then review the tally outcomes of each pair of pairs using homomorphic encryption. If an untruthful tally is found, step 3 is repeated until no further untruthful totals can be seen, at which point the couple in question is labeled as dishonest. A no tally, no vote' principle to deter malicious or deliberate 'go-out' actions in the counting stage is followed. If a peer fails to carry out the count, he will be listed as a deceptive peer, and all votes will be cast out. The premise is that a truthful colleague will record a tally outcome with adequate time.

4 Results And Discussion

First, the suggested technique identifies fraudulent activity without a reliable third party. It can recognize both straightforward individual-on-individual cheating as well as dynamic collaborative cheating by a range of different co-workers. A single peer may exhibit a level of compliance disproportionate to others. Section III details the kind of actions taken by lone-wolf fraudsters that would be considered violations of

the proposed protocol. It is easy to see how solo cheating behaviors may be recognized, whether carried out by a trustworthy peer or via intelligent contracts. This segment displays how the detected cheating may be addressed without a responsible party to avoid altering the vote result. Cooperative Fraud is a more complicated kind of Smart Agreement, and on Chain, using some fraud scheme in this segment demonstrates how this can be accomplished. To attain this goal, it is necessary to invalidate any votes cast by peers that violate ethical standards. This goal may be efficiently performed by deleting votes from the recording stage after first identifying them as "invalid" and then designating them as such. Second, colleagues who fail to uphold ethical standards must be excluded from the counting process. This is a much more challenging scenario. This same action constitutes the revocation.

This permits equal counterparts to vote formerly encrypted votes by dishonest peer HEPKj, i.e., allow them to vote instead by a truthful peer HEPKj-encrypted replacement bulletin. It can guarantee that corrupt peers can no longer decode legitimate votes by revoking them and that it is thus disqualified immediately from the count. If a peer is not matching appropriately, then it will detect him. After enough time has passed, the peer's counted votes will be invalidated, re-examined, and counted again by trustworthy peers. By correctness of the referendum's outcome, the correct total of all votes means the result. (1) The overall tally result does not include an invalid ballot; (2) all valid votes are correctly counted and used. The consistency of the suggested protocol can be seen immediately from the abovementioned detectability and correctness. Furthermore, the transparency and auditability of voting data, such as public keys to the electors, votes, records, count results, status updates, etc., are assured because it is all registered tamper-proof by the blockchain chief. The protocol preserves the secrecy of a vote with "distribution votes" and encryption.

The K votes cast by each voter in this scheme will be encrypted using a random selection of K public keys, and the voters' m ballot selections will be dispersed among all K ballots. This ensures that each vote is encrypted and sent securely using the public key of a single pair. Furthermore, up to the limit, only a certain number of pairings say b pairs, may report voting b ballots. The voter's choice is always revealed if b is more minor than 0.5k. Therefore, if b is enormous and the necessary fault tolerance limit is high for improved privacy security, K should not be tiny. Future research is needed to nail down K for b. In this voting system's protocol, voters are presumed to be peers in a blockchain-based network.

In a blockchain that has been authorized or in a blockchain that does not have permission, the identities of co-workers may be utilized to guarantee that they are eligible to vote. This is because being a co-worker on the network does not incur any insignificant expenses. The identification of the pairs and the public key are both used in the regulation of the voting individual's authentication process. Other situations where the list of voters is appropriately handled by a blockchain or a group of users with access control inside the group in the public Blockchain are also applicable to this protocol. Moreover, it applies to circumstances of a grander scale. Because of the relatively large number of fraudulent votes, sophistication may be an issue. This is because many identification and rectification aspects rely on clever agreements, par-

ticularly the verification system. In addition, votes, revokes, and counts for impacted ballots must be redone if a new unethical peer is discovered.

When everything is said and done, if a dishonest counter is discovered, the result is thrown away to revoke it and tell others about the votes it has counted. Because of this, his votes need to be thrown out, which means that the simple counters who were impacted will need to throw away the ballots and pay for this counter. Practical approaches such as voting, and counter-separation may be taken to reduce uncertainty. It is anticipated that more research will resolve this issue shortly. For the evaluation, accuracy, throughput, and latency parameters are chosen to prove the extraordinary performance of the proposed blockchain-based e-voting framework. Figure 2, Figure 3, and Figure 4 show the accuracy, throughput, and latency analysis of the proposed e-voting framework, respectively.

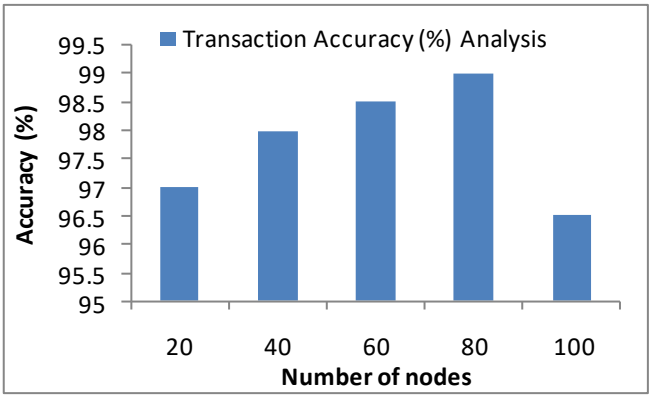

Fig. 2. Transaction accuracy analysis for the proposed E-Voting framework.

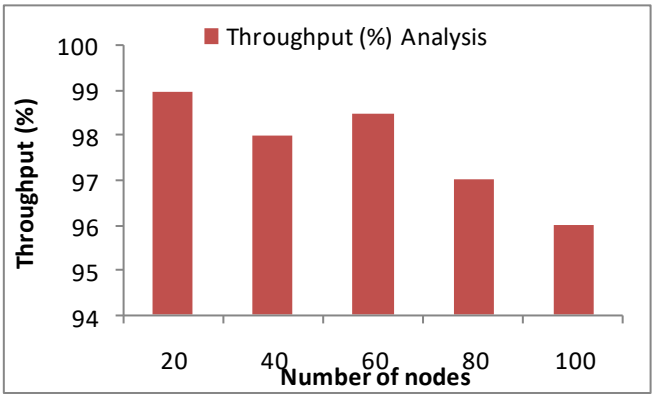

Fig. 3. Throughput analysis for the proposed E-Voting Framework.

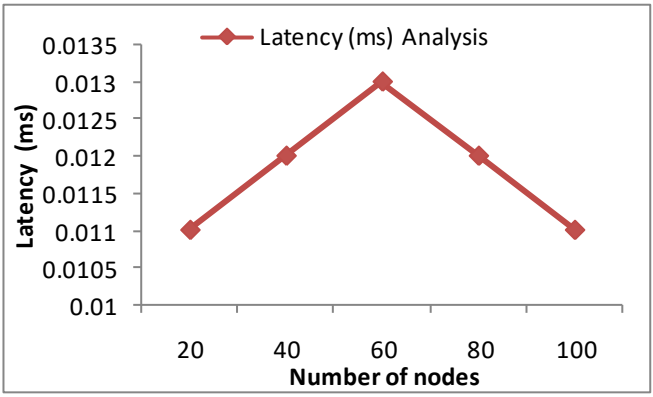

Fig. 4. Latency analysis for the proposed E-voting framework.

It is observed that the proposed framework maintains 96.5% and 99% transaction accuracy. Figure 4 shows that the peak throughput achieved is 99%, and in Figure 5, the latency is minimized for all node densities. So, increasing node density will not affect the system performance in terms of throughput and accuracy. The proposed framework synchronization speed is very high and improves the overall performance of the e-voting framework.

5 Conclusion

In this article, a proposal is made to make it easier for peers on a blockchain to ascertain the results of voting using a native blockchain mechanism. The suggested procedure safeguards voters' rights while making it simpler to identify corrupt practices and take corrective action without a reliable partner. This hyper-ledger implementation fabric demonstrates that a protocol for voting on small to larger-scale topics is realistic and realizable. The adequacy of the suggested framework is shown concerning the precision of the transactions, the throughput, and the latency. In the future, additional labor will need to be performed. First, there must be an official evaluation of the security measures. It is essential to investigate all potential threats to the defense, such as an assault by the cartel on the design. Second, it is crucial to do a theoretical investigation of the system characteristics, including the number of votes and the duration of the main PKI. Thirdly, the voting mechanism is being implemented to conduct tests in the real world. In the future, further analysis is anticipated to be undertaken to test and refine. It can enforce the protocol on numerous public and consortium blockchain networks.

References

1. Balasubadra, K., Shadaksharappa, B., Seeni, S. K., Sridevi, V., Thamizhamuthu, R., Srinivasan, C.: Real-time Glass Recycling Quality Assurance and Contamination Reduction

with IoT and Random Forest algorithm. International Conference on Inventive Computation Technologies, 1788-1793. (2024).
2. Kumar, T. R., Enireddy, V., Selvi, K. K., Shahid, M., Babu, D. V., Sudha, I.: Fractional chef-based optimization algorithm trained deep learning for cardiovascular risk prediction using retinal fundus images. Biomedical Signal Processing and Control, 94, 106269. (2024).
3. Komathi A., Kishore S.R., Velmurugan A.K., Begum A.S., Muthukumaran D.: Network load balancing and data categorization in cloud computing. Indonesian Journal of Electrical Engineering and Computer ScienceThis link is disabled, 35(3), 1942-1951(2024).
4. Nasreen A.K., Shenbagapriya M., Seeni S.K., Veda P., Meenakshi B., Muruganm S.: Robotic Restroom Hygiene Solutions with IoT and Recurrent Neural Networks for Clean Facilities. International Conference on Inventive Computation Technologies, 1842-1847, 2024.
5. Lakshmi, D., Varadarajan, M. N., Nithisha, J., Sivakamy, N., Prakash, S.: Decision Trees for Secure and Transparent Equipment Failure Prediction in Cloud-Connected Manufacturing. 10th International Conference on Communication and Signal Processing. 1211-1216. (2024).
6. Karthikeyan, C., Kumar, T. R., Babu, D. V., Baskar, M., Jayaraman, R., Shahid, M.: Speech enhancement approach for body-conducted unvoiced speech based on Taylor–Boltzmann machines trained DNN. Computer Speech and Language, 83, 1-9 (2023).
7. Pravin Kumar, M., Jayaraman, T., Senthilkumar, M., Sumaiya Begum, A.: Performance Investigation of Generalized Rain Pattern Absorption Attention Network for Single-Image Deraining. Journal of Circuits, Systems and Computers, 32(13), 1-12 (2023).
8. Umamaheswari, K., Rajan, D. A. J., Ramasamy, J., Seeni, S. K., Meenakshi, R., Thamizhamuthu, R.: SVM-Guided Dynamic Routing for Post-Harvest Quality Preservation in Smart Warehouses with IoT. 3rd International Conference for Innovation in Technology. 1-6. (2024).
9. Senkamalavalli1 R., Sankar S., Parivazhagan A., Raja R., Selvaraj Y., Porandla Srinivas P., Naarayanasamy Varadarajan M.: Enhancing clinical decision-making with cloud-enabled integration of image-driven insights. Indonesian Journal of Electrical Engineering and Computer Science, 36 (1), 38-346. (2024).
10. Akbar, S. B., Thanupillai, K., Sundararaj, S.: Combining the advantages of AlexNet convolutional deep neural network optimized with anopheles search algorithm-based feature extraction and random forest classifier for COVID-19 classification. Concurrency and Computation: Practice and Experience, 34(15), 1-15 (2022).
11. Anitha, P., Ranganathan, C. S., Babiyola, A., Jafersadhiq, A.: Decision Tree Algorithm for Intelligent Resource Management in Wireless Networks. Second International Conference on Augmented Intelligence and Sustainable Systems, 1396-1400 (2023).
12. Selvi T, K., Sumaiya Begum, A., Poonkuzhali, P., Aarthi, R. Brain tumor classification for MRI images using dual-discriminator conditional generative adversarial network," Electromagnetic Biology and Medicine, 43 (1-2), 81-94 (2024).
13. Ravinder, B., Seeni, S. K., Prabhu, V. S., Asha, P., Maniraj, S. P., Srinivasan, C.: Web Data Mining with Organized Contents Using Naive Bayes Algorithm. 2nd International Conference on Computer, Communication and Control, 1-6 (2024).
14. Raman, R., Peter, J. B. J., Gokhale, A. A., Manikandan, J., Ganesh, E. N., Srinivasan, C.: Implications of Brewer's Rule in Data Warehouse Design 7th International Conference on I-SMAC, 349-354 (2023).
15. Srinivasan, S., Veda, P., Asha, P., Srinivasan, C., Murugan, S., Sujatha, S.: SVM Classifier in IoT-Connected Doorway Thermal Scanning for Preventive Health Check Surveillance.

1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems, 1-6 (2024).
16. Begum, A. S., Poornachandra, S.: Curvelet based image de-noising using beta-trim shrinkage for magnetic resonance images. International Conference on Science Engineering and Management Research, pp. 1-8, 2014.
17. Sindhumitha, K., Jeyachitra, R. K., Manochandar, S.: Joint modulation format recognition and optical performance monitoring for efficient fiber-optic communication links using ensemble deep transfer learning. Optical Engineering, 61(11), 116103-116103 (2022).
18. Raman, R., Dhivya, K., Sapra, P., Gurpur, S., Maniraj, S. P., Murugan, S.: IoT-driven Smart Packaging for Pharmaceuticals: Ensuring Product Integrity and Patient Safety. International Conference on Artificial Intelligence for Innovations in Healthcare Industries, 1, 1-6 (2023).
19. Premalatha, P., Muthukumaran, K., Jayabalan, P.: Experimental study on behaviour of piles in berthing structure. In Proceedings of the Institution of Civil Engineers-Maritime Engineering, 168(4), 182-193 (2015).
20. Karthikeyan, A., Vanitha, N. S., Meenakshi, T., Ramani, R., Murugan, S.: Electric Vehicle Battery Charging in Grid System using Fuzzy based Bidirectional Converter. 3rd International Conference on Innovative Mechanisms for Industry Applications, 1447-1452 (2023).
21. Premalatha, P. V., Kumar, S. S., Baskar, K.: Influence of change in pile diameter at various locations of a pile group in a Berthing Structure. Indian Journal of Geo-Marine Sciences, 46(6),1198-1209 (2017).
22. Jegan, J., Suguna, M. R., Shobana, M., Azath, H., Murugan, S., Rajmohan, M.: IoT-Enabled Black Box for Driver Behavior Analysis Using Cloud Computing. International Conference on Advances in Data Engineering and Intelligent Computing Systems, 1-6. 2024.
23. Shanthi, S., Kannan, B. M., Babuji, R., Sivakumar, S., Malathi, N.: Optimizing City Transit: IoT and Gradient Boosting Algorithms for Accurate Bus Arrival Predictions. 2nd IEEE International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, 1-5, (2024).
24. Srinivasan, S., Indra, G., Saravanan, T. R., Murugan, S., Srinivasan, C., Muthulekshmi, M.: Revolutionizing Skin Cancer Detection with Raspberry Pi-Embedded ANN Technology in an Automated Screening Booth. 4th International Conference on Innovative Practices in Technology and Management, 1-6 (2024).
25. Rajarajan, S., Kowsalya, T., Gupta, N. S., Suresh, P. M., Ilampiray, P., Murugan, S.: IoT in Brain-Computer Interfaces for Enabling Communication and Control for the Disabled. 10th International Conference on Communication and Signal Processing, 502-507 (2024).
26. Lenin, J., Komathi, A., Vijayan, H., Rathinam, A. R., Kasthuri, A., Srinivasan, C.: Revolutionizing Healthcare With Cloud Computing: The Impact of Clinical Decision Support Algorithm. International Conference on Artificial Intelligence for Innovations in Healthcare Industries ,1-6 (2023).
27. Balasubadra, K., Shadaksharappa, B., Seeni, S. K., Sridevi, V., Thamizhamuthu, R., Srinivasan, C.: Real-time Glass Recycling Quality Assurance and Contamination Reduction with IoT and Random Forest algorithm. International Conference on Inventive Computation Technologies, 1788-1793 (2024).