IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 9, 2021, accepted September 19, 2021, date of publication September 23, 2021, date of current version October 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3115238

Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server

B. SOWMIYA[1], E. POOVAMMAL[1], (Senior Member, IEEE), KADIYALA RAMANA[2], (Member, IEEE), SAURABH SINGH[3], AND BYUNGUN YOON[3], (Senior Member, IEEE)

[1]School of Computing, SRM Institute of Science and Technology, Chennai, Tamil Nadu 603203, India
[2]Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences (AITS), Rajampet 516126, India
[3]Department of Industrial and Systems Engineering, Dongguk University, Seoul 10326, South Korea

Corresponding author: Saurabh Singh (saurabh89@dongguk.edu)

This research was supported by a grant (21163MFDS502) from the Ministry of Food and Drug Safety, Korea, in 2021.

ABSTRACT Cloud computing is a continuously evolving technology that can enhance agility, availability, collaboration and scalability of data. Blockchain has a secure, immutable ledger which maintains all the transactions along with the timestamp. The blockchain framework and cloud computing technology jointly provides different ways of computational cost reduction. The existing methods help to identify the anonymous documents which are given in the form of requests from the cloud server. If the anonymized document requests are from the authorized users, then cloud provides better security and hence documents are not available for unauthorized users. But the main issue is access rights available for authorized users on sensitive data of the owner. To maintain the privacy the sensitive data are hidden using cryptographic techniques even for authorized users. The method adopted is Linear Elliptical Curve Digital Signature (LECDS) with Hyperledger blockchain, to prevent private data loss. The Linear regression method is used to classify the user information into two classes namely sensitive and non-sensitive. The non-sensitive data is encrypted using RSA and sensitive data is encrypted using LECC method. Modified Spider optimization search Algorithm (MSOA) is used to verify the integrity of outsourced data and search user query information in a cloud server. The hyper ledger blockchain verifies the user policy to create a private network through which the user communicates the cloud. In the analysis of the proposed method, the results are evaluated using various performance metrics such as security, throughput, classification accuracy and error rate.

INDEX TERMS Hyperledger blockchain, modified spider search, cloud computing.

I. INTRODUCTION

Blockchain is a distributed ledger that records time series transactions. The general ledger is maintained with server update transactions of all the participating node. Blockchain enforces trust by doing validation process (Merkel tree) on each transaction that has been hashed with transparency and which makes the transactions to become immutable [1]. Blockchain eliminates the risk of a single point of failure because it is distributed in nature, and every network node makes a copy of the transaction data. Blockchain guarantees the integrity of transactions. Hence faster transaction happens between two parties without mediation.

There are two main categories of Blockchain technology: Permission less and granting permission. Permission less blockchains, commonly referred to as public blockchains, are open to all users [2]. However, existence of huge potential public blockchain like Bitcoin, may not be suitable for all business owners who want to control transaction processing systems. Business processes can participate in the complex operations along with customized solutions and then limit outsiders who have specific requirements and needs. Some challenges in permission less blockchains are scalability, regulatory and control evolution as the size of the chain increases. The companies which want to have personal

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Abdur Razzaque.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

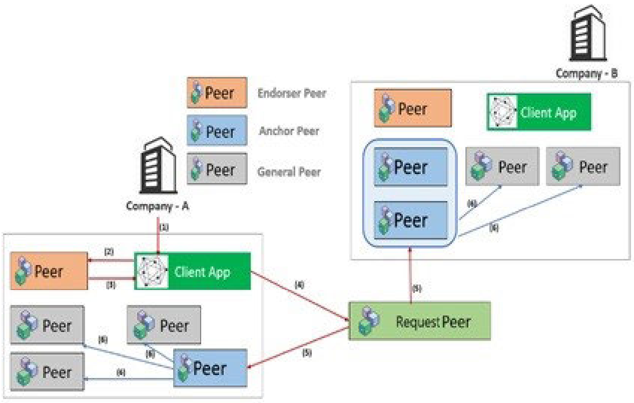

FIGURE 1. Hyperledger fabric blockchain architecture.

control to empower and allow only trusted parties to join the blockchain network started exploring other option. The blockchain that grants permissions is also called a private blockchain [3].

Trust operators want them to process and maintain transaction records accurately and securely. Since the operation is mainly manual, there is also the possibility of loopholes and fraud in daily transactions. As a result, we cannot guarantee the integrity and reliability of many businesses. Hyperledger is an effort to collaborate on cross-industry blockchain technologies which helps to create and promote open source. The Hyperledger deployment platform can provide a highly confidential, flexible, and extensible degree to support distributed ledger solutions using the architecture shown in figure 1.

There are various threats and attacks that need to be addressed when we incorporate blockchain. The most common attack called 51% attack happens in blockchain network when one party holds more control over the network but when we use Hyperledger fabric it is a private permissioned blockchain where the participants in the network have limited access to data than the organization head. The second type of attack that commonly exist in blockchain network is sybil attack. The sybil attack are imposed to degrade the reputation of the system by creating a large no. of pseudonymous identities. The proposed model tries to eliminate the sybil attack by authenticating and validating the identities using the elliptic curve digital signatures.

The elliptic curve code is widely used to protect mini automated devices. Not only in secret securitizing and allocation of just text but the images and more of the multimedia content also be secured with ECC. Therefore, ECC-based cryptology research is an emerging interdisciplinary area which is combined with the growing fields like mathematics, electronic, electrical and computer science.

II. RELATED WORK

The section II discusses the earlier methods, which presents the security issues related to blockchain cloud storage. The author [4], assumes n as number of companions and f is the maximum of the malicious nodes, Hyperledger proposes to enable PeerBFT to handle Byzantine failures in the fabric sorting service. The paper clearance management is proposed by the Emergency Access Control Management System (EACMS) based on Blockchain hyperledger fabric and hyperledger composer [5]. Data Items the organization suggested regarding the use of emergency and term smart contracts may specify certain restrictions to limit patients' health achievement (PHR) permissions and define certain rules. Licensing management of PABC is based on the blockchain international patent application system. Patent applications may be modified or rejected without reliance on the patent office [6]. The management system Professional Node in every patent office in a country or region feels contracted for all applications. The literature [7] proposes a distributed authentication infrastructure called the Meta Indonesian Communist Party, through which multiple certificate authorities (CAs) can cross-certify algorithms such as exchange mechanisms.

A dynamic joint consensus project authority to verify and validate event data effectively by new modules without any authority center [8]. It conducts numerical analysis and, based on it, proposes a quick leader election algorithm and Hyperledger Cloth Blockchain Network emulator test. A new Blockchain-based Reliable and Intelligent Animal Information Management System (RIVIMS) has been suggested for smart contracts and the use of machine learning technology [9], [10]. Blockchain is based on standard veterinary information management, data and forecast analysis modules. It is necessary to examine two of the four aspects of manufacturing and research systems: distributed ledger, cryptography, consensus protocol, and smart contract [11]. The data processing workload is the framework for understanding the performance of private blockchains. Common software failures and blockchain-specific software failures [12] (e.g., the need for a transaction sender) affect the reliability and integrity of the Smart Contract Index and observations of absolute reliability.

The consumer node uses electronic energy converters to develop consumer profiles and consumption profiles for smart meters [13], [14] in a real-life situation. Platform collectors use permissions to enable the data owner to ensure that only designated parties can process personal data and use smart contracts and encryption technology to record all data transactions within a standard distributed bargain. Provides a new method [15] to address the shortcomings of the existing centralized system. In the paper [16], the Permit Management Blockchain based on the Hyperledger-based Emission Trading System (HyperETS) is proposed. A measuring instrument used in shared blockchain-based constructions [17]. The conceptual model is compared to the distributed measurement model discussed in the previous measurement tools and previous work.

The [18] article explores the ongoing multi-party use of private data security supported by the multi-party computation (MPC) Fabric. In the solutions, pioneers use MPC to store their data from the series before encryption and whenever such private data protection is required. The security properties of the sorting mechanism [19], [29] and the influence of late authentication messages on the federation's blockchain protocol. Damage to the attacker can lead to news of honest players who are delayed by subsequent hit evidence. Blockchain [20] degree supplier management inventory sharing facility can be designed to design scientific research methods based on the Hyperledger fabric software model.

Then, the smart contract starts to calculate the basics and supports the possibility of adaptive load that can meet the needs of each customer; Blockchain will record customer energy consumption or generation [1], [21]. The client-side should be aware of the deployment address of chain code [22] and endorsement policies within the platform. In past releases, this was statically configured on the client-side. Blockchain data integration-based programs can successfully avoid the problem of trusting third-party protocols [2], [23], but they must face major computational and overhead communication issues. This low security makes it difficult to provide different types of data classification for sensitive and non-sensitive user information. Some more information on blockchain, cloud computing, privacy preserving and data storage security are accessed in ref [1], [2], [24]–[38].

III. IMPLEMENTATION OF THE PROPOSED METHOD

The elliptic curve digital signatures algorithms (ECDSA) are used as the basis for bitcoin security. The key feature of ECDSA is shorter key length with high degree of security similar to RSA. The proposed Linear Elliptical Curve Digital Signature (LECDS) with hyperledger blockchain framework provides security for sensitive and non-sensitive information from a cloud database using shorter key length. The proposed Linear Elliptical Curve Digital Signature (LEADS) with hyperledger blockchain framework provides security for sensitive and non-sensitive information from a cloud database. The cloud security method first classifies the user information before cloud storage. Data classification is determined based on the availability, integrity, and confidentiality of the security target and the data classification's sensitivity. Data owners must monitor the data throughout its life cycle and carefully analyze each piece of data to determine the potential impact of unauthorized leakage or destruction of these data. Symmetric key generation to provide a public key for each data for service verification.

Broken access control is one of the security metrics that is considered in the LECDS model because nowadays in many applications the authentication is done after the login verification. So, there is a chance that the even authorized or unauthorized users will be able to see the content which they are not allowed to see. To eliminate this drawback before saving the content to the cloud the LECDS encrypt the data and then store in the cloud. The LECDS also provides system security metric which is two layers of security. The non-sensitive data encryption to secure using an RSA method, and sensitive data are encrypted using an LECC method. The user request key and user policy are verified after the Information is encrypted.

The process of the proposed block diagram is present in figure 2. Modified Spider search optimization algorithm help to search the user request query information from the cloud. Once the policy is verified, all user query transactions are stored on a hyper ledger, and a private network cloud blockchain is created to request the user. In this data security framework, authorized users only can access both sensitive and non-sensitive data.

A. MODIFIED SPIDER SEARCH OPTIMIZATION

SSO expects the entire query space to be search query information, where all spiders communicate with each other. In this way, each array in space asks about the location of the cloud feature. All inquiries received by the spider are conformity estimates placed by social spider representatives. The updated spider is updated again with the help of Drosophila optimization algorithms to achieve better query selection. This algorithm designs two distinctive inquiry operators (spiders): sensitive and non-sensitive Information to update the user query population. Each interaction is operated by various development operators who follow the unique, effective behaviors typically expected within the state. By characterizing the total amount of n-dimensional individuals, characterize the quantity of sensitive and non-sensitive spiders in the whole population F using the equation 1.

$$\begin{aligned} N_q &= ds[0.9 - rend(0,1) * n] \; and \; N_{sq} \\ &= n - n_{ns} \end{aligned} \tag{1}$$

where the N_q User query and N_{sq} user sequence query and n = number of query information

B. FITNESS EVALUATION

Spider size is the trademark that assesses the individual ability to perform better than its allotted undertakings. Each user (spider) gets a feature (query) F_i which indicates the arrangement quality that compares to the spider i (independent of Information) of the populate F. Fit (F_i) is the fitness value received by estimating the spider location F_i concerning the objective function F and the values $worst_q$, and $best_q$ are computed utilizing the below expression.

Spider size is a trademark that evaluates an individual's ability to work better than its assigned cause. Each user (spider) gets a feature (query) F_i that indicates the quality of the permutations. It is compared to fill-in F_i. Approximate (F_i) If the spider i (independent Information) is the fitted value F_i received by estimation, the relative spider position of the objective function F and the values $worst_q$ and $best_q$ are using the fitness function.

C. MODELING OF THE VIBRATIONS THROUGH THE COMMUNAL QUERY

Public queries are used as a mechanism for sending Information between colony members. This Information is encoded

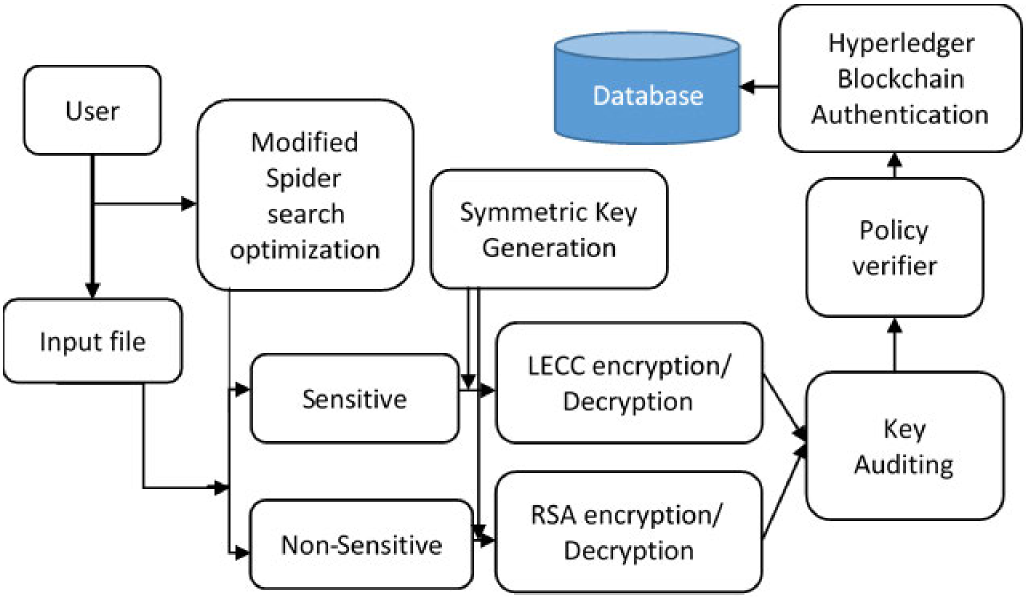
User
Modified Spider search optimization
Symmetric Key Generation
Database
Hyperledger Blockchain Authentication
Policy verifier
Input file
Sensitive
Non-Sensitive
LECC encryption/ Decryption
RSA encryption/ Decryption
Key Auditing

FIGURE 2. Proposed method block diagram.

as a small vibration that is the key to the collective coordination of all individuals in the group. The quality of Information depends on the weight and distance of the spiders they are producing. Individuals nearby have a stronger perception of vibrations than those who are far away, as distance-induced vibrations and their relatives to the detection components. To reproduce this process, the personal vibration perception (equation 2) i is the result of the Information sent by the authorized user j according to the following equation:

$$vib_{ij} = w_i f^{-d_{ij}} \tag{2}$$

where the d_{ij} is the Euclidian distance (equation 3) between the spiders i and j, such that

$$d_{ij} = F_i - F_j \tag{3}$$

The algorithm starts by instating the set F of N spider locations every spider location f_{si}, and m_{si} is a dimensional vector consisting of the parameter qualities to be improved. Such values are arbitrarily and consistently dispersed between the pre indicated low beginning parameter limit p_j^{high}. The higher primary value limit p_j^{high} similarly as it conveyed by utilizing equation.

D. SYMMETRIC KEY GENERATION

The proposed method creates a private key S_k, controlling or creating a key on the cloud at the user's request. The keys in the cloud obtain by encrypting the sensitive and non-sensitive data. For each user request to verify in key auditing to allow the user. Authentication is a mechanism provided by the host to check the integrity of the data stored in the cloud. Well-known organizations for data authentication add MACs to their data.

E. ALGORITHM

```
Input: NULL
Output: Service Key Set SKS.
Initialize Service set $S_s$.
Identify the set of all services available.
$SS = \sum Service \in Network$
For each service $S_i$ from $S_s$
Initialize service I'd SID.
Compute maximum bytes of streams to remain attached.
$M_s = Bandwidth/(size(S_s))ServicePriority$
If data ==S
Generate Encryption key $E_k$ and encrypt using elliptic curve cryptography.
Else if data ==NS
Generate Encryption key $E_k$ and encrypt using RSA.
$C_s$=compute the current size of the stream using prime factor.
$SID = SID + MS + CS$.
Perform Encryption Cipher using Encrypt (SID, $E_k$).
Store Cipher, SID, $E_k$ to the key set.
SKS = Cipher, SID, $E_k$.
End
```

The ECC, RSA logarithm problem (ECDLP) using a polynomial-time bounded algorithm is hard. In addition, a 160-bit size ECC-based key offers the same level of security as obtained using 1024-bit RSA-based key generation.

F. HYPERLEDGER FABRIC BLOCKCHAIN

The Hyperledger fabric's anatomy is to obtain a blockchain network with authority set by the tissues trying to form the consortium. Each component unit in the blockchain network is responsible for configuring the network in which the peer participates. All these peers' needs consist of certification

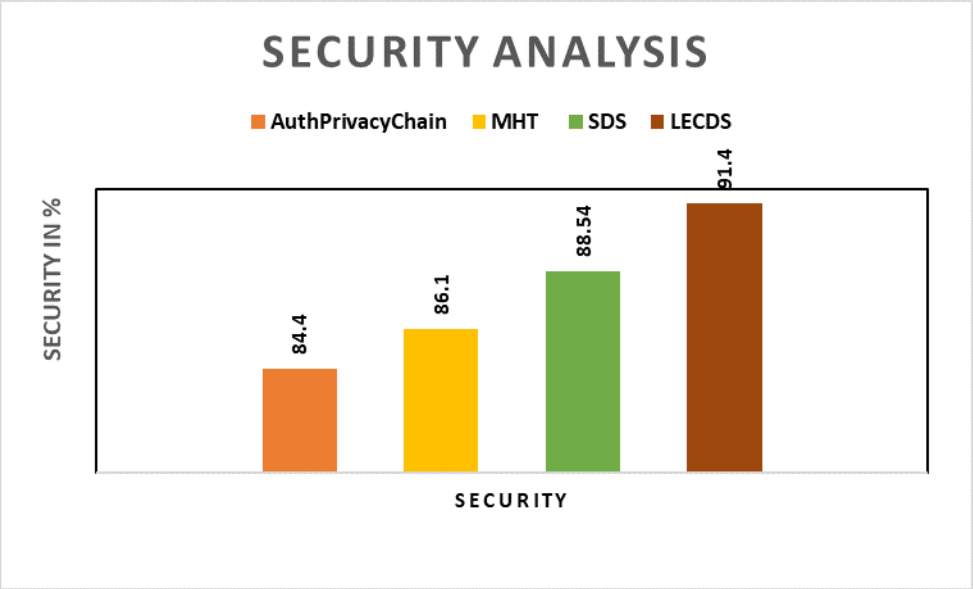

FIGURE 3. Comparison of security analysis.

authorities and other Information similar to the appropriate cryptographic material.

- Membership Services Provider: Enrolls the clients
- *Peers:* Peer nodes can be endorser (endorse the proposal for the transaction) and committer nodes (write block of transactions to the ledger)
- *Chaincode:* Peer nodes having chain code becomes the endorser for that chain code. ESCC (Endorser system chain code) executes the chain code using read-write set information.

Hence Distributed Ledger Technology (DLT) to maintain all the user records. In this hyperledger fabric blockchain following building block and flow is present in the figure. Generations within the membership organization receive customer transaction call requests from within the organization. The client can be any particular sensitive file for a particular application/service portal. All peers maintain their accounts per channel, and they subscribe.

G. EXPERIMENTAL SETUP

We used virtual machine 3.5GHz, 4 Core Processor, 128 GB RAM, 1 TB Hard disk. We have used adult dataset(ics.uci.edu/ml/datasets/Adult). The total no. of instances is 48842. The sensitive and non-sensitive attribute distribution on the above-mentioned dataset was easy since the attribute chosen are common attributes for different applications like medical, educational, etc . . .

IV. RESULTS AND DISCUSSION

This method aims to improve the fact that it has a significant impact on security and mental accuracy, the time complexity of user roles, and secure access to cloud environments. A tool in the Microsoft .net Framework for SQL Server databases generates test cases with appropriate user access to access private and public users throughout the configuration design process. Users can trust access and permissions to thousands of files, demonstrating the high impact of the evaluation department on privacy issues. The manual attacks where imposed and checked against, how far the attackers were able to adapt to the security controls in the environment. The proposed LECDS methods shows 91.4% of security for different types of manual penetration testing attacks that were imposed on the system. The proposed Linear Elliptical Curve Digital Signature (LECDS) method is compared to the existing AuthPrivacyChain, MHT (Merkle Hashing Tree) method and SDS (Stochastic Diffusion Search). In this analysis of security result proposed method LECDS provides a 91.4% security compare to existing methods MHT has 86.1%, AuthPrivacyChain has 84.4%, security in the medical blockchain network. Figure 3 represents the comparison of the proposed and existing method graph.

This analysis result shows that the proposed LECDS method has a low time delay than existing AuthPrivacyChain and MHT methods. Figure 4 present the proposed LECDS method comparison of execution time analysis. The hyper ledger blockchain creates a private channel for each user and provides security for each data transaction. So the proposed method LBSK provides better performance.

The proposed LECDS method of throughput analysis comparison is shown in figure 5. The spider optimization Search reduces the user search time and improves the throughput when several transactions are processed compared to the existing method. This proposed LECDS method of transaction performance provides a 700tps (transaction per second) higher rate for 500 transactions than the existing method AuthPrivacyChain provides a 650tps lower rate.

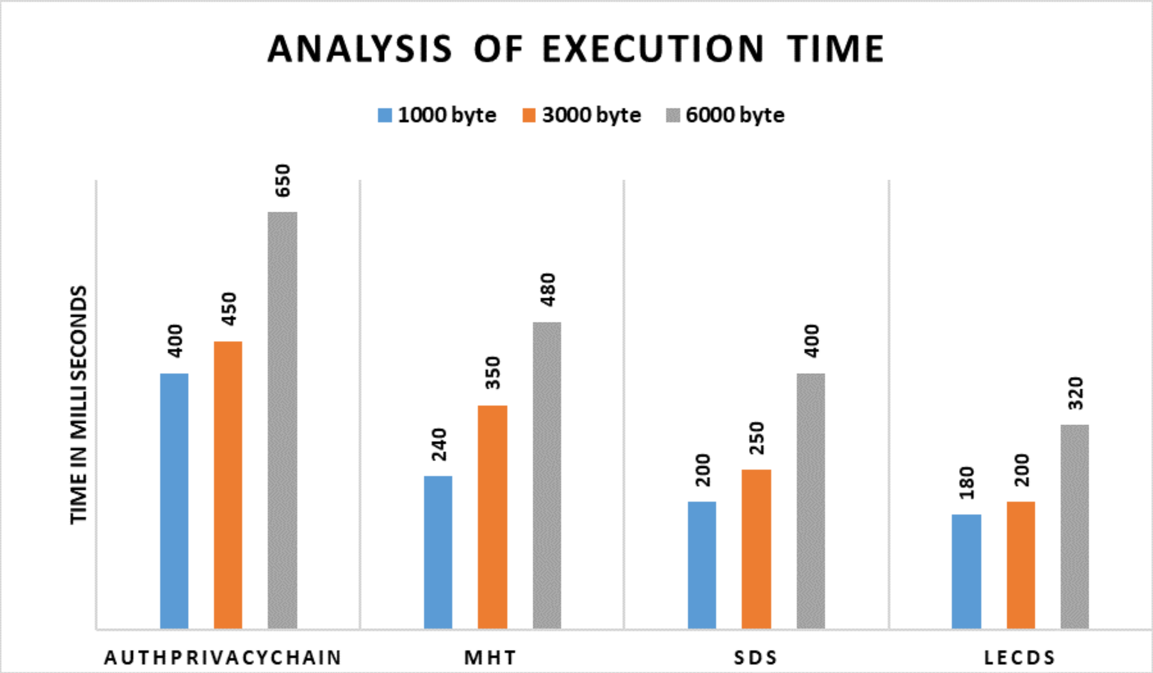

FIGURE 4. Analysis of execution time.

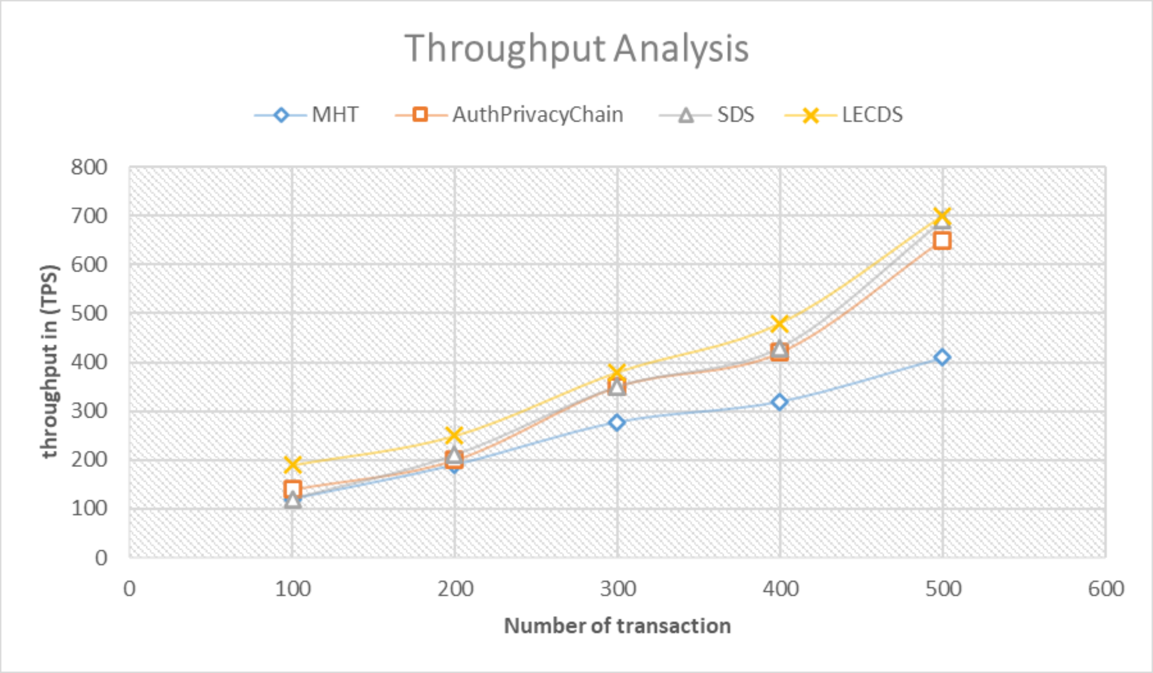

FIGURE 5. Comparison of throughput analysis.

In this analysis of the proposed LECDS method, results provide 0.21% of low misclassification for 150blocks compared to the existing method. In this comparison of the proposed method, LECDS existing method SDS, MHT and AuthPrivacyChain provide a higher misclassification rate there are shown in figure 6.

The analysis on average latency performance has been measured and presented in Figure 7, where the proposed LECDS algorithm has produced lower latency performance than other methods. In this result, the proposed LECDS method 0.6 for 2sec for the transaction. Similarly, AuthPrivacyChain provides 0.98sec, the MHT method has 1.22sec, and the SDS method has 07sec. In this average latency analysis result of the proposed method, LECDS provides a lower latency rate compared to other existing methods.

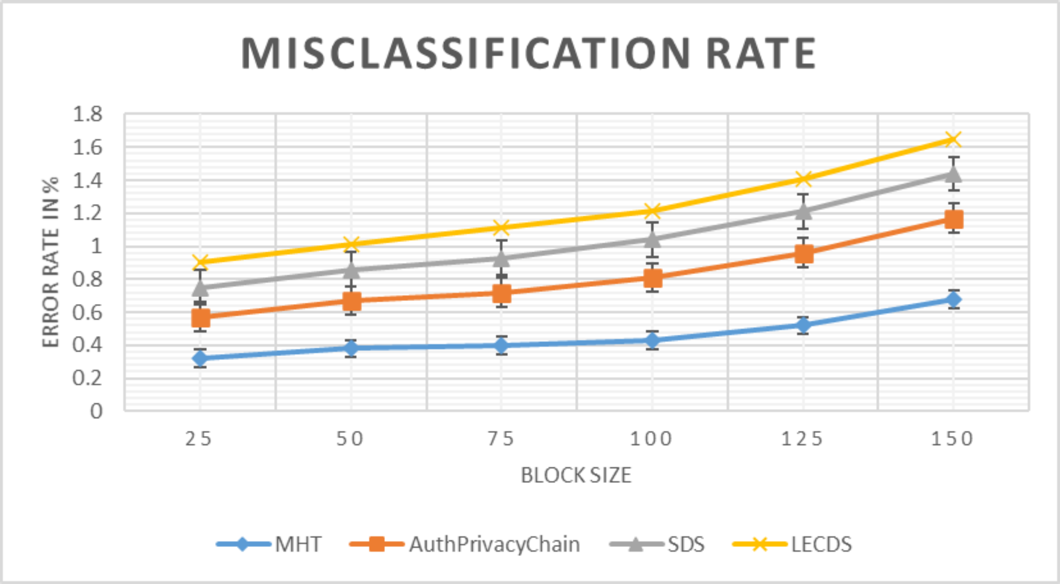

FIGURE 6. Misclassification performance analysis.

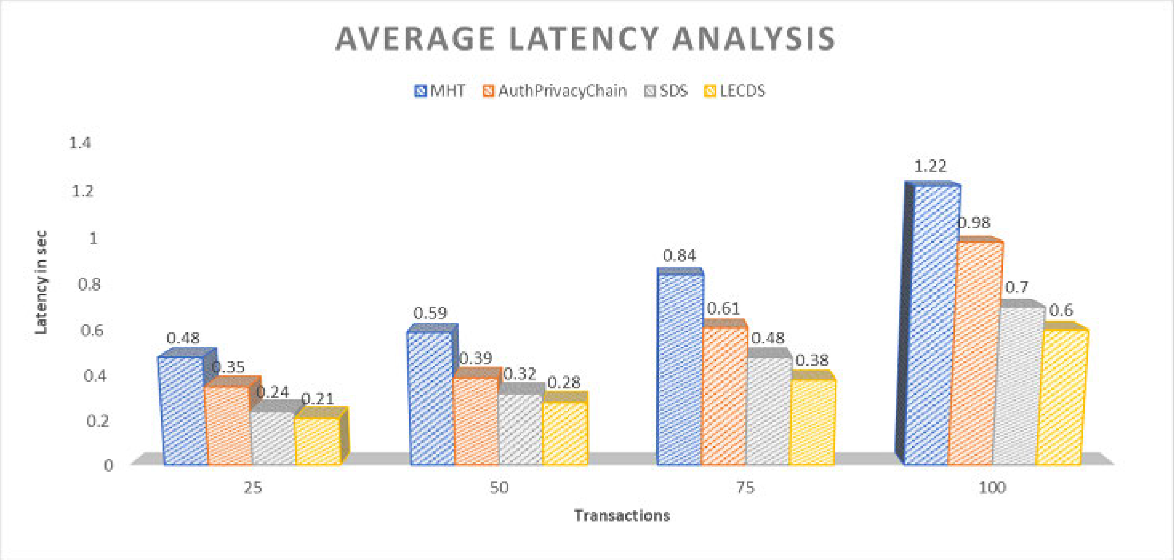

FIGURE 7. Average latency analysis.

V. CONCLUSION

Ensuring digital data security during storage and transmission is a great challenge faced by the digital society. New encryption schemes are needed to withstand new forms of attacks. RSA and LECC cryptography is an emerging field in cryptography and can produce strong encryption algorithms. The detailed study of the conventional symmetric encryption schemes and RSA-based cryptographic algorithms led to the development of a novel RSA-based Symmetric Cipher. This proposed hyper ledger blockchain provides a higher security performance and classifies the sensitive and non-sensitive data from the cloud. The sensitive data will encrypt using an ECC method and RSA algorithm used to encrypt non-sensitive data. This hyper plan encryption method provides efficient, stronger security. The SSO method is used to search the user query and fastest transaction query processing in the blockchain network. This overall proposed method LECC method, provides better performance compared to another existing method. Although this work has addressed security, privacy and usefulness, the limitations are cost and time taken to split and encrypt the sensitive and non-sensitive data in Hyperledger platform. We have further planned to work on other blockchain platform like midchain by comparing the security and performance metrices of Hyperledger.

REFERENCES

[1] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, "A secured distributed detection system based on IPFS and blockchain for industrial image and video data security," *J. Parallel Distrib. Comput.*, vol. 152, pp. 128–143, Jun. 2021.

[2] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, ''Security and privacy of UAV data using blockchain technology,'' *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102670.

[3] D. S. Rajput, P. Shukla, T. Reddy, R. Kaluri, K. Lakshmanna, P. K. R. K. Maddikunta, and H. Patel, ''A review on bitcoin and currency encryption: Bitcoin and blockchain,'' *Blockchain Applications in IoT Security*. Hershey, PA, USA: IGI Global, 2021, pp. 84–98.

[4] J. Ma, Y. Jo, and C. Park, ''PeerBFT: Making hyperledger fabric's ordering service withstand byzantine faults,'' *IEEE Access*, vol. 8, pp. 217255–217267, 2020, doi: 10.1109/ACCESS.2020.3040443.

[5] A. R. Rajput, Q. Li, M. T. Ahvanooey, and I. Masood, ''EACMS: Emergency access control management system for personal health record based on blockchain,'' *IEEE Access*, vol. 7, pp. 84304–84317, 2019, doi: 10.1109/ACCESS.2019.2917976.

[6] S. Bian, G. Shen, Z. Huang, Y. Yang, J. Li, and X. Zhang, ''PABC: A patent application system based on blockchain,'' *IEEE Access*, vol. 9, pp. 4199–4210, 2021, doi: 10.1109/ACCESS.2020.3048004.

[7] S. Kakei, Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimoto, and S. Saito, ''Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric,'' *IEEE Access*, vol. 8, pp. 135742–135757, 2020, doi: 10.1109/ACCESS.2020.3011137.

[8] H. Guo, W. Li, M. Nejad, and C.-C. Shen, ''Proof-of-event recording system for autonomous vehicles: A blockchain-based solution,'' *IEEE Access*, vol. 8, pp. 182776–182786, 2020, doi: 10.1109/ACCESS.2020.3029512.

[9] N. Iqbal, F. Jamil, S. Ahmad, and D. Kim, ''A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services,'' *IEEE Access*, vol. 9, pp. 8069–8098, 2021, doi: 10.1109/ACCESS.2021.3049325.

[10] B. Huang, L. Jin, Z. Lu, X. Zhou, J. Wu, Q. Tang, and P. C. K. Hung, ''BoR: Toward high-performance permissioned blockchain in RDMA-enabled network,'' *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 301–313, Mar. 2020, doi: 10.1109/TSC.2019.2948009.

[11] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, ''Untangling blockchain: A data processing view of blockchain systems,'' *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[12] A. Hajdu, N. Ivaki, I. Kocsis, A. Klenik, L. Gonczy, N. Laranjeiro, H. Madeira, and A. Pataricza, ''Using fault injection to assess blockchain systems in presence of faulty smart contracts,'' *IEEE Access*, vol. 8, pp. 190760–190783, 2020, doi: 10.1109/ACCESS.2020.3032239.

[13] G. Sciume, E. J. Palacios-Garcia, P. Gallo, E. R. Sanseverino, J. C. Vasquez, and J. M. Guerrero, ''Demand response service certification and customer baseline evaluation using blockchain technology,'' *IEEE Access*, vol. 8, pp. 139313–139331, 2020, doi: 10.1109/ACCESS.2020.3012781.

[14] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, ''GDPR-compliant personal data management: A blockchain-based solution,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2020, doi: 10.1109/TIFS.2019.2948287.

[15] P. Yuan, X. Xiong, L. Lei, and K. Zheng, ''Design and implementation on hyperledger-based emission trading system,'' *IEEE Access*, vol. 7, pp. 6109–6116, 2019, doi: 10.1109/ACCESS.2018.2888929.

[16] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, ''A blockchain-based privacy-preserving authentication scheme for VANETs,'' *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019, doi: 10.1109/TVLSI.2019.2929420.

[17] W. S. Melo, A. Bessani, N. Neves, A. O. Santin, and L. F. R. C. Carmo, ''Using blockchains to implement distributed measuring systems,'' *IEEE Trans. Instrum. Meas.*, vol. 68, no. 5, pp. 1503–1514, May 2019, doi: 10.1109/TIM.2019.2898013.

[18] F. Benhamouda, S. Halevi, and T. Halevi, ''Supporting private data on hyperledger fabric with secure multiparty computation,'' *IBM J. Res. Develop.*, vol. 63, no. 2/3, pp. 3:1–3:8, Mar. 2019, doi: 10.1147/JRD.2019.2913621.

[19] T. Meng, Y. Zhao, K. Wolter, and C.-Z. Xu, ''On consortium blockchain consistency: A queueing network model approach,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 6, pp. 1369–1382, Jun. 2021, doi: 10.1109/TPDS.2021.3049915.

[20] T. Guggenberger, A. Schweizer, and N. Urbach, ''Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology,'' *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1074–1085, Nov. 2020, doi: 10.1109/TEM.2020.2978628.

[21] M. L. Di Silvestre, P. Gallo, E. R. Sanseverino, G. Sciumè, and G. Zizzo, ''Aggregation and remuneration in demand response with a blockchain-based framework,'' *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4248–4257, Aug. 2020, doi: 10.1109/TIA.2020.2992958.

[22] Y. Manevich, A. Barger, and Y. Tock, ''Endorsement in hyperledger fabric via service discovery,'' *IBM J. Res. Develop.*, vol. 63, no. 2/3, pp. 2:1–2:9, Mar. 2019, doi: 10.1147/JRD.2019.2900647.

[23] H. Wang and J. Zhang, ''Blockchain based data integrity verification for large-scale IoT data,'' *IEEE Access*, vol. 7, pp. 164996–165006, 2019, doi: 10.1109/ACCESS.2019.2952635.

[24] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj, and A. Tolba, ''Data secure storage mechanism of sensor networks based on blockchain,'' *Comput., Mater. Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.

[25] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, ''A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles,'' *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.

[26] J. Wang, W. Chen, Y. Ren, O. Alfarraj, and L. Wang, ''Blockchain based data storage mechanism in cyber physical system,'' *J. Internet Technol.*, vol. 21, no. 6, pp. 1681–1689, 2020.

[27] J. Zhang, S. Zhong, J. Wang, X. Yu, and O. Alfarraj, ''A storage optimization scheme for blockchain transaction databases,'' *Comput. Syst. Sci. Eng.*, vol. 36, no. 3, pp. 521–535, 2021.

[28] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj, and A. Tolba, ''Data secure storage mechanism of sensor networks based on blockchain,'' *Comput., Mater. Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.

[29] T. Wang, Y. Quan, X. S. Shen, T. R. Gadekallu, W. Wang, and K. Dev, ''A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things,'' *IEEE Trans. Ind. Informat.*, early access, Aug. 10, 2021, doi: 10.1109/TII.2021.3103547.

[30] S. Singh, A. S. M. S. Hosen, and B. Yoon, ''Blockchain security attacks, challenges, and solutions for the future distributed IoT network,'' *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[31] M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan, N. Herencsar, and J. C.-W. Lin, ''Enhancing security of health information using modular encryption standard in mobile cloud computing,'' *IEEE Access*, vol. 9, pp. 8820–8834, 2021.

[32] J. Wang, W. Chen, L. Wang, Y. Ren, and R. S. Sherratt, ''Blockchain-based data storage mechanism for industrial Internet of Things,'' *Intell. Autom. Soft Comput.*, vol. 26, no. 5, pp. 1157–1172, 2020.

[33] J. Mei, K. Li, Z. Tong, Q. Li, and K. Li, ''Profit maximization for cloud brokers in cloud computing,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 1, pp. 190–203, Jan. 2018.

[34] B. L. Nguyen, E. L. Lydia, M. Elhoseny, I. V. Pustokhina, D. A. Pustokhin, M. M. Selim, G. N. Nguyen, and K. Shankar, ''Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data,'' *Comput., Mater. Continua*, vol. 65, no. 1, pp. 87–107, 2020.

[35] C. Liu, K. Li, K. Li, and R. Buyya, ''A new service mechanism for profit optimizations of a cloud provider and its users,'' *IEEE Trans. Cloud Comput.*, vol. 9, no. 1, pp. 14–26, Jan. 2017.

[36] Y. Yan, Y. Dai, Z. Zhou, W. Jiang, and S. Guo, ''Edge computing-based tasks offloading and block caching for mobile blockchain,'' *Comput., Mater. Continua*, vol. 62, no. 2, pp. 905–915, 2020.

[37] S. Singh, Y.-S. Jeong, and J. H. Park, ''A survey on cloud computing security: Issues, threats, and solutions,'' *J. Netw. Comput. Appl.*, vol. 75, pp. 200–222, Nov. 2016.

[38] R. Song, Y. Song, Z. Liu, M. Tan, and K. Zhou, ''GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism,'' *Comput. Mater. Continua*, vol. 60, no. 3, pp. 973–987, 2019.

B. SOWMIYA received the B.E. degree in computer science and engineering from Anna University Affiliated College, Chennai, India, and the M.Tech. degree in advance information and technology from Bharadhidasan University, India. She is currently pursuing the Ph.D. degree in blockchain with SRM Institute of Science and Technology, Chennai. Her research interests include data mining, machine learning, and information security. She is a member of professional bodies ACM, IET, and ISCA.

E. POOVAMMAL (Senior Member, IEEE) received the B.E. degree in electrical and electronics engineering, in 1990, the M.E. degree in computer science and engineering, and the Ph.D. degree in computer science and engineering, in 2011. She is currently a Professor with the Department of Computer Science and Engineering and the Associate Director (Campus life) at SRM Institute of Science and Technology. In 1996, she joined SRM. Prior to that, she was working in industry for more than five years. She has published more than 60 articles in refereed journals and presented in various international and national conferences. Her research interests include data mining, big data analytics, and machine learning. She is a fellow of IE(I). She is a Life Member of ISTE and Indian Science Congress. She is a member of other professional bodies IET, ACM, and CSI. She was a recipient of the Best Academic Dean Award by the Association of Scientists, Developers and Faculties (ASDF), in 2015, and the Women Engineer Award by IET-CLN, in 2013.

KADIYALA RAMANA (Member, IEEE) received the Bachelor of Technology degree in information technology from JNTUH, Hyderabad, India, the M.Tech. degree from Satyabhama University, Chennai, India, and the Ph.D. degree from SRM University, Chennai. He is currently working as an Associate Professor with the Department of Artificial Intelligence and Data Science, AITS, Rajampet, India. He has 14 years of experience in teaching and research. He has authored more than 20 international publications. His research interests include wireless sensor networks, software-defined networking with machine learning, and data analytics. He is an editorial board member and a reviewer of several journals of international repute.

SAURABH SINGH received the Ph.D. degree from Jeonbuk National University, Jeonju, South Korea, carrying out his research in the field of ubiquitous security. He was a Postdoctoral Researcher with Kunsan National University, South Korea. He currently joined as an Assistant Professor with Dongguk University, Seoul, South Korea. He has published many SCI/SCIE journals and conference papers. His current research interests include blockchain technology, cloud computing and security, the IoT, deep learning, and cryptography. He received the Best Paper Award from KIPS and CUTE Conference, in 2016.

BYUNGUN YOON (Senior Member, IEEE) is currently a Professor with the Department of Industrial and Systems Engineering, Dongguk University. His theme of study has involved blockchain technology, patent analysis, new technology development methodology, and visualization algorithms. His current research interests include enhancing technology road mapping, research and development quality, and product designing with data mining techniques.