ISSN 2347 - 3983

Volume 8. No. 9, September 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter188892020.pdf

https://doi.org/10.30534/ijeter/2020/188892020

Authentication based Data Access Control and sharing mechanism in Cloud using Blockchain Technology

Yogesh M. Gajmal[1], Udayakumar R.[2]

[1]Research Scholar, Department of CSE, BIST, BIHER, Chennai,India,yogeshmgajmal@gmail.com

[2]Professor, School of Computing Sciences, BIST, BIHER, Chennai, India, rsukumar2007@gmail.com

ABSTRACT

Cloud computing is an innovative developing technique. The cloud surrounding is a big open distributed scheme. It is essential to preserve the information, along with, confidentiality of users. Access control stays single of vital tools for ensuring safety of information. It guarantees that legal user's access the information and the system. It is identify users trying to access a system illegally. It is a technique which is desperately essential for security in computer. Outmoded access mechanism skills by means of discretionary access mechanism, identity-based access mechanism, stand not appropriate on behalf of applying access mechanism in Internet of Things methods. One more mutual technique mandatory access control (MAC) is normally required via a vital supervisor, which remains problematic in single-opinion fail. In this paper we propose a new authentication also access control mechanism in cloud used for data sharing based on block chain Technology. However, the system involves of two different things, as Data Owner (DO), and Data User (DU). The DU makes the enrollment demand using the authentication and sends it to DO, which processes the demand and verifies the DU. The performance of the proposed method is measured using the metrics, like better Genuine user detection rate of 95% and Memory usage of 1580 kbps with the Blockchain of 100-500 size, respectively.

Key words: Blockchain, Data sharing, Security, Authentication, Ethereum.

1. INTRODUCTION

Through the fast growth of internet tools, cloud storing has turn into an significant professional prototypical inside our regular time. This one has delivered diverse varieties of information storing facilities for entities also originalities, creating it likely for customers to right to use Internet assets plus share information by anytime and everywhere, it has took great opportuneness towards our survives. The appearance of the blockchain takes permitted us in the direction of connects the P2P cryptocurrency through storing space, bandwidth, CPU control, etc. [8]. The blockchain stays a scattered design that arrangements a scattered unchallengeable ledger inside which wholly communications stands documented. Additional, blockchain residues a protected also distributed information collection of systematic records, together with events, called blocks [9]. Now the outmoded cloud storing method, the mysteries of only spot of letdown jerry can resolution through procedure of distributed storing method then enjoy several benefits in excess of central storing scheme [8]. Decentralized information is kept taking place each only peer of the realm, and not single can modify that one. Hash of information stays created towards kind of variability difficult. The Blockchain scheme be there basically strong then consumes no only weakness intended on behalf of hacker towards abuse. Blockchain scheme archives the data see-through to every node; also this one stays seeming to fill in the information, that's why blockchain remain trustworthy [1]. The blockchain tools make available everybody using an in work evidence of a distributed faith. Entire cryptocurrencies make use of whatever can best remain defined by way of a open ledger that remains hard towards immoral. Each particular customer then node has the flawless similar ledger as for each whole of the extra customers otherwise nodes inside the scheme. This assurances a entire contract after each customers otherwise nodes inside the equal coins blockchain [4].

It stays an exposed, see-through and scattered ledger that record trades among two sides professionally in a provable and long-lasting technique [11]. As soon as make a note, the information going on the blockchain cannot remain interfered except a novel agreement is touched. Merging IoT through blockchain skill remains a capable tendency then is probable to confirm faith as well as decrease complete overhead on behalf of IoT schemes. That one can assistance IoT towards establishes a distributed, trustworthy and in public provable record as a result that billions of linked belongings can accomplish a scattered faith finished it [2]. In the direction to permit information holder to individual also regulator their individual information, an single data organization system constructed going on blockchain tools continued established in [12], the scheme can come to be improved defense of the confidentiality of customer's information. In direction toward resolve the problematic of information confidentiality, a blockchain construction scheme was established [13], inside attribute-based encryption skill is use to appliance information access mechanism. Aimed at the determination of resolving the safety also confidentiality glitches that delay growth of big information, a blockchain centered access mechanism arrangement used going on behalf of increasing the safety of big information stages [10] was presented [8]. Access control stands the finest vital tools for assuring the safety of data. Old-fashioned access mechanism apparatuses such in place of discretionary access mechanism, identity-based access mechanism, stand not appropriate aimed at applying access mechanism in IoT schemes, since that one is nearly difficult to create an access mechanism list used aimed at everyone at the present the IoT scheme going on version of the massive amount of unidentified individualities [2].

Access mechanism is that restrictions the processes otherwise actions of a genuine user. The access mechanism functionalities rise through integration of allocation unit, wherever the allocation is a procedure for allocating provisional consents toward a customer [5]. Additional shared method mandatory access mechanism is usually compulsory via a significant supervisor, which occurs the problematic of single-point disappointment. By way of IoT strategies may have its place to diverse management administrations toward whether their position or purpose, centralized access mechanism method does not appropriate for IoT schemes. Attribute-based access mechanism delivers a kind of elastic, active and fine-grained access mechanism. It summaries the parts or else the individualities keen on a established of characteristics give out by the characteristic experts. An access rule defined by a Boolean formulation above a set of characteristics is used towards defines the legal and official access. Here is no extended necessity to allocate roles otherwise create access mechanism lists for everyone in the scheme. As an alternative, the attribute experts simply requirement to achieve each characteristic well-defined in the method then allot them to appropriate customers. In this technique, access administration can be efficiently streamlined as per the amount of characteristics is much fewer than the amount of customers in the scheme [2].

The significant contribution of this study is described as follows

- The proposed access control and data sharing method has the capability of distributing the secret keys to the data users and states the access rules in direction to encrypt the shared data. Still, the search utility of the distributed system is assessed with the smart contract of Ethereum blockchain.

Rest of article is presented as per follow: Section 2 describes literature survey plus challenges. Section 3 explains proposed Blockchain-based access mechanism also data distribution procedure. Section 4 explains the results and discussion of proposed method and section 5 conclude the article.

2. MOTIVATION

Here, different existing access control methods and blockchain-based access methods are surveyed, which inspire the researchers to change a new technique to improve the security of data.

2.1 Literature survey

Rajput, A.R et al. [1] proposed Emergency access control management system (EACMS). This frame offers superior effectiveness associated thru the outmoded emergency access method. But the time efficiency of this model was very poor.
Ding, S et al. [2] designed Attribute-based access control scheme. It is effectively resists several attacks in addition to are professionally applied now in IoT methods and it was not suitable for the fine-grained access control scheme.
Ma, M et al. [3] presented Blockchain-based distributed key management approach. This approach is the vibrant transaction collection period alteration permits the performance in addition to scheme capability to be enhanced for different surroundings. However, it failed to simplify the persistency of the blockchain-based Internet of Things ecosphere.
Ouaddah, A et al. [4] introduce Decentralized pseudonymous as well as secrecy preservative authorization organization structure. This framework effectively managed the access control going on behalf of constrained strategies. However, it unable to implement the Fair Access with Raspberry PI IoT device and bit coin blockchain.
Ali, G et al. [5] proposed Distributed design on behalf of consent allocation plus access mechanism. This model attained better confidentiality, integrity and availability and this model was failed toward effort in proper demonstrating in addition prescribed confirmation of BC.
Dagher, G.G et al.[6] presented Blockchain-based framework. This framework attains an elevated of distributed although admitting that several nodes should toward of a higher power. However, methodologies still propose important confidentiality protection also data truthfulness.
Lin, C et al. [7] designed Blockchain-based method used for safe mutual verification. This scheme provides confidentiality and safety assurances such as unidentified verification, auditability, and privacy. But then it unsuccessful to enhance the performance with hardware application, also work together by a smart workshop worker.
Wang, S et al. [8] presented Blockchain-Based Framework. This framework attained high throughput with reduced cost. However, this model failed to implement the roles of customer's characteristic withdrawal also access rule modernize.
Sastry, JKR et al. [14] Open Stack equipment fine grained Scheme well-defined controls are intended for affecting the access mechanism towards the customer information. Every single user well-defined through the well-designed accountabilities which stay toward addressed through customer roles, which stand providing certain access privileges through the capability towards create certain procedures regarding the assets providing into Open Stack.
Tatyana Deeva, Galina et al. [15] it is suggested in the direction of consider a smart agreement such as a kind of contract with a superior technique aimed at its conclusion, which creates it promising in the direction of put on it into the practice, with the current tools of contractual directive. Nevertheless, due to the nonexistence of legal rules, judicial security of the privileges of the parties toward a smart contract is not certain through act.

2.2 Challenges

In [13], privacy-preserving blockchain architecture was developed toward discourse the privacy problems in the IoT requests. Even although blockchain provisions reliability in addition to non-repudiation to specific level, secrecy also confidentiality of the information otherwise the strategies remain not well-preserved.
In [7], secure mutual authentication mechanism was introduced in the direction of apply fine-grained access control strategy. This approach was planned on the way to offer secrecy and safety assurances such as unidentified verification, auditability, and privacy. It influences the behind features of blockchain is different cryptographic resources to understand a distributed, privacy-protective also auditable resolution.
In [10], Blockchain-based access control was demonstrated to provision the safety of Big Data. It usages idea of blockchain in addition to breakdown the tool and philosophies of the access control structure. It influences the main structures of Blockchain that be there, scattering, complete and append-only ledger towards create a auspicious resolution used for addressing abovementioned access control contests happening in Big Data. A distributed individual information organization scheme was developed in [12] to guarantee users personal in addition to control their information. IT knows the customers by way of the

proprietors of their private information. It tie together them addicted to an experienced answer for trustworthy calculating glitches in the humanity.

Data storing and distribution system was introduced to allocate secret key with data users, then encode shared information thru stating access strategy. This system succeeds fine-grained access control above information. It was more feasible, but failed to implement the roles of customer's characteristic withdrawal in addition access strategy modernize [8].

3. PROPOSED METHODOLOGY

The main purpose of this work is to design and develop a novel authentication as well as access control mechanism in cloud on behalf of data sharing based on block chain. This work designs a model for the mutual authentication of the data user and data owner in the system. However, the scheme contains of double different things, by way of data owner, and data user. Data Owner (DO) stands the individual or association that possesses a sequence of records to distribute. Data User (DU) is the data clients of the data owner that are authorized to view some of the file. The proposed authentication and access control framework involves eight different phases, namely setup, user registration, encrypt, token gen, control setup, test, validation, and decrypt. The setup phase stays run through the DO, which takings the contribution as the safety limit and generates the system master key and public parameter. The Data Owner encodes the master key then implants in keen on an Ethereum contract. The customer registering phase is track by Data Owner. That one taking the scheme master key as input also generates the output secret key. In the encrypt phase, the files are encrypted using the encryption algorithm, by taking the shared file as input. It generates the ciphertext, file encrypt key, also keyword fixed from the file. Next, the tokengen phase is executed to generate the search token. The control setup is the additional phase used in this proposed data sharing framework. The test phase returned the relevant transaction id and the success key matching results. The results are validated and verified in the validation phase. Finally, the decrypt phase decrypts the encrypted file by the decryption algorithm. Moreover, the implementation of this work will be carried out in PYTHON, and the performance of the proposed algorithm will be evaluated using the evaluation metrics, like bandwidth and responsiveness. Finally, the proposed method will compare with the existing techniques, like EACMS [1], Attribute-based access control [2], and BSeIn [7]. Figure 1 displays block diagram of proposed authentication and access control mechanism.

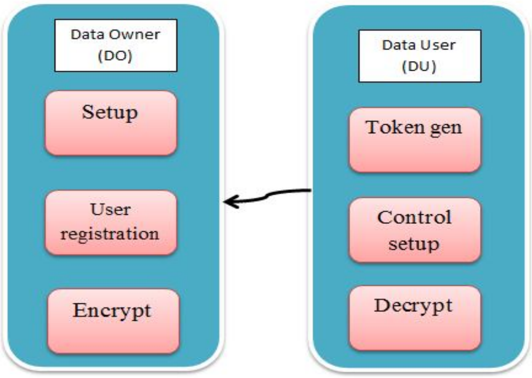

Figure 1: Block diagram of access control and authentication in cloud

4. RESULTS AND DISCUSSION

The results and discussion of the proposed access control and data sharing methodology is described here.

4.1 Experimental setup

The research of the projected cloud model is carried out in the PYTHON tool by windows 10 OS, 4 GB RAM, plus Intel processor.

4.2 Evaluation metrics

The performance of the projected method is assessed with metrics, such as Genuine user detection rate and Memory Usage.

Genuine user detection rate: It is labeled as the number of users detected as genuine by respect to the entire total of users.

Memory usage: It is defined as the memory available in system is the sum of total memory installed in system.

4.3 Comparative methods

The performance enhancement of the proposed method is discovered by comparing the proposed with the existing techniques, like Emergency Access Control Management System (EACMS) [1], Attribute-Based Access Control (ABAC) [2], and blockchain-based scheme (BSeIn) on behalf of distant mutual verification [7], respectively.

4.4 Comparative analysis

The comparative analysis of the projected Blockchain-based access mechanism also information distribution approach stands complete via the performance metrics, such as Genuine user detection rate and Memory Usage by varying the blockchain size.

A. Blockchain size=100

Figure 2 a) portrays the comparative analysis of the proposed approach with the Blockchain size as 100. Figure 2 a) represents the comparative analysis of Genuine user detection rate with respect to the number of users. By considering 20 number of users, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 65.7%, 65.76%, and 58.46%, while the proposed Blockchain based access mechanism and data distribution obtained better Genuine user detection rate of 95%, respectively. When number of users=40, the Genuine user detection rate obtained by the proposed Blockchain based access mechanism also data distribution is 75.16%, while the percentage of improvement reported when comparing the proposed with the existing methods, like ABAC, BSeIn, EACMS is 14%, 28%, and 46%, respectively. When the number of users=60, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 51.15%, 50.10%, and 42%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 65.76%, respectively. When number of users=80, the Genuine user detection rate obtained by the proposed Blockchain based access mechanism also information sharing is 58.46%, while the percentage of improvement reported when comparing the proposed with the existing methods, like ABAC, BSeIn, EACMS is 16%, 33%, and 94%, respectively. When the number of users=100, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 33.40%, 30%, and 30%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 58.46%, respectively.

Figure 2 b) depicts the comparative analysis of responsiveness through detail toward amount of users. When users are 20, then memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 1615.88kbps, 1729.93kbps, and 1733.65kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 1583.97kpbs, respectively. When the number of users=40, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 1638.78kbps, 1733.75kbps, and 1758kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 1786.88kbps, respectively. When the number of users=60, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 1782.99kbps, 1663.39kbps, 1759.64kbps, while the proposed Blockchain based access mechanism also information sharing obtained lower responsiveness of 1614.24kbps, respectively. When the number of users=80, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 1809.29kbps, 1690.66kbps, 1780.23kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 1634.83kbps, respectively. When the number of users=100, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 1865.16kbps, 1806.58kbps, 1740.23kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 1657.40kbps, respectively.

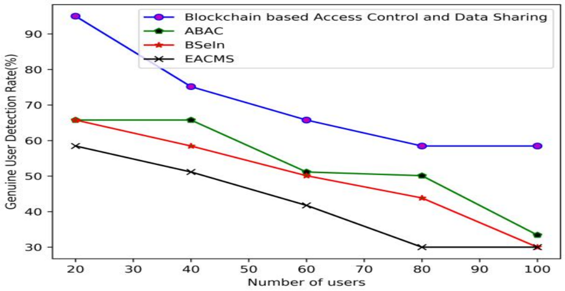

Figure 2 a): Comparative analysis with the Blockchain size as 100, Genuine user detection rate

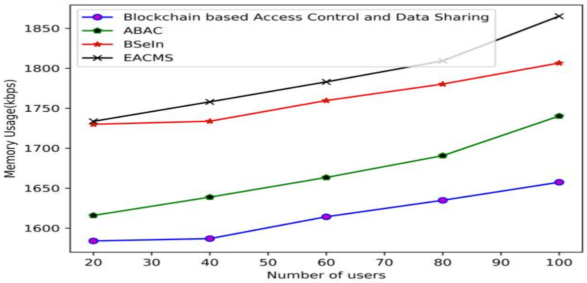

Figure 2 b): Comparative analysis with the Blockchain size as 100, Memory usage

B. Blockchain size=200

Figure 3 a) portrays the comparative analysis of the proposed approach with the Blockchain size as 200. Figure 3 a) represents the comparative analysis of Genuine user detection rate. When the number of users=20, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 83%, 70%, and 38%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 95%, respectively. When the number of users=40, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 70%, 52%, and 30%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 83%, respectively. When number of users=60, the Genuine user detection rate obtained by the proposed Blockchain based access mechanism also data distribution is 54%, while the percentage of improvement reported when comparing the proposed with the existing methods, like ABAC, BSeIn, EACMS is 15%, 81%, and 81%, respectively. When the number of users=80, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 30%, 30%, and 30%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 35%, respectively. Figure 3 b) depicts the comparative analysis of memory usage. When the number of users=20, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 3648.87kbps, 3504.85kbps, and, 3414.88kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 3347.84kbps, respectively. When the number of users=40, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 4172.63kbps, 3939.39kbps, and 3909.08kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 3757.29kbps, respectively. When the number of users=60, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is4231.48kbps, 4016.86kbps, and 3959.24kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 3880.68 kbps, respectively. When the number of users=80, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is4328.23kbps, 4079.36kbps, and 4045.22kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of3902.06kbps, respectively.

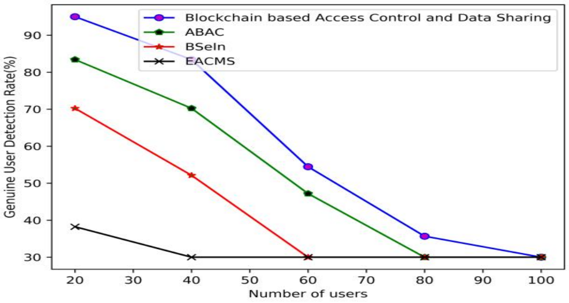

Figure 3 a): Comparative analysis with the Blockchain size as 200, Genuine user detection rate

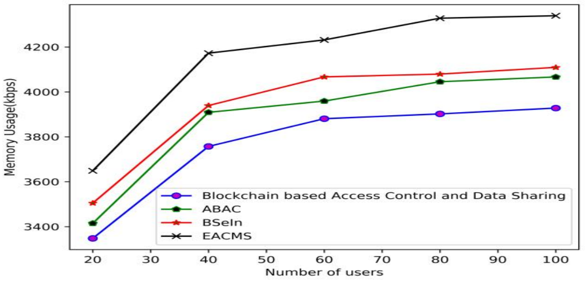

Figure 3 b): Comparative analysis with the Blockchain size as 200, Memory usage

C. *Blockchain size=300*

Figure 4 a) portrays the comparative analysis of the proposed approach with the Blockchain size as 300. Figure 4 a) represents the comparative analysis of Genuine user detection rate through admiration toward amount of users. When users are =20, then Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 75%, 69%, 68%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 95%, respectively. When the number of users=40, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 61%, 56%, 56%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 73%, respectively.

Figure 4 b) depicts the comparative analysis of memory usage. When the number of users=20, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 5303.02kbps, 4980.77kbps, and, 4950.63kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 4827.99kbps, respectively. When the number of users=40, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 5454.31kbps,5096.05kbps, and 5041.64kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of4886.17kbps, respectively. When the number of users=60, the memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is 5684.82kbps, 5219.75kbps, and 5245.60kbps, while the proposed Blockchain based access control and data sharing obtained lower memory usage of 5081.41 kbps, respectively.

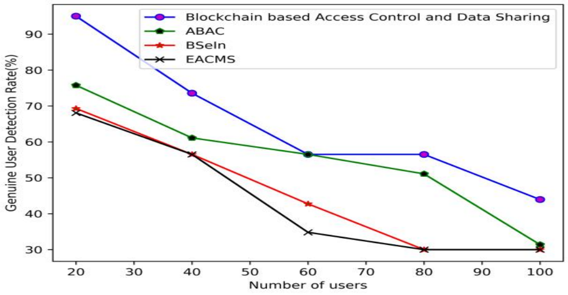

Figure 4 a): Comparative analysis with the Blockchain size as 300, Genuine user detection rate

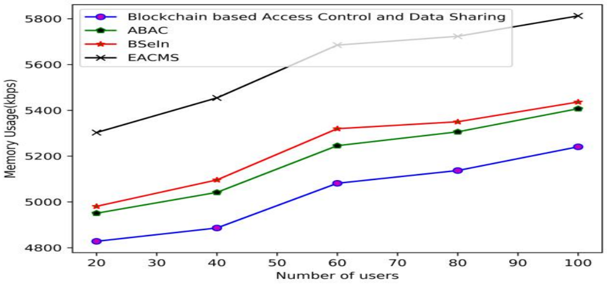

Figure 4 b): Comparative analysis with the Blockchain size as 300, Memory usage

D. *Blockchain size=400*

Figure 5 a) portrays the comparative analysis of the proposed approach with the Blockchain size as 400. Figure 5 a) represents the comparative analysis of Genuine user detection rate with number of users. By considering 20 number of users, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 83%, 83%, 61%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 95%, respectively.

Figure 5 b) depicts the comparative analysis of Memory usage to number of users. When the number of users=20, the Memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS is5618.05kbps, 5755.68kbps, and 5887.59kbps, while the proposed Blockchain based access control and data sharing obtained lower Memory usage of 6332.93kbps, respectively.

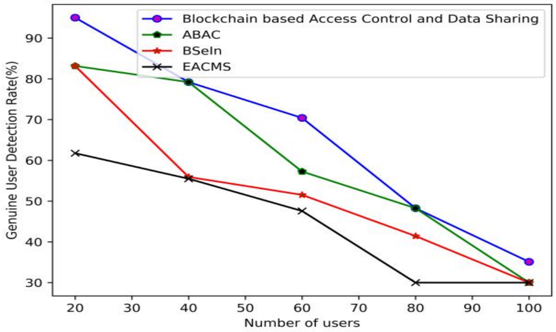

Figure 5 a): Comparative analysis with the Blockchain size as 400, Genuine user detection rate

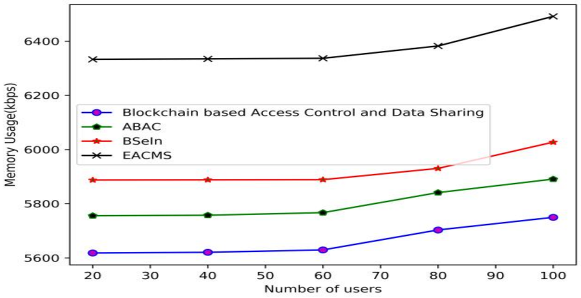

Figure 5 b): Comparative analysis with the Blockchain size as 400, Memory usage

E. Blockchain size=500

Figure 6 a) portrays the comparative analysis of the proposed approach with the Blockchain size as 500. Figure 6 a) represents the comparative analysis of Genuine user detection rate to number of users. For 20 users, the Genuine user detection rate obtained by the existing methods, such as ABAC, BSeIn, EACMS is 61%, 57%, 49%, while the proposed Blockchain based access control and data sharing obtained better Genuine user detection rate of 95%, respectively.

Figure 6 b) depicts the comparative analysis of Memory usage to number of users. When the number of users=20, the Memory usage obtained by the existing methods, such as ABAC, BSeIn, EACMS, 8346.04kbps, 8507.45kbps, and 8656.83kbps, while the proposed Blockchain based access control and data sharing obtained lower Memory usage of is 8346.04kbps, respectively.

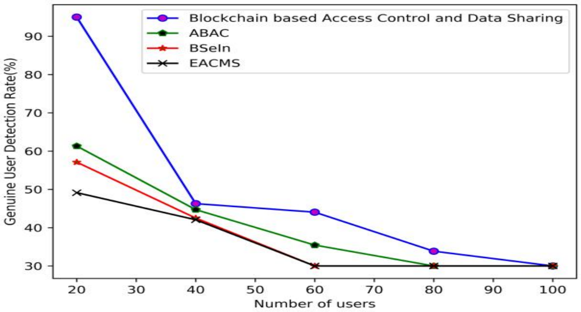

Figure 6 a): Comparative analysis with the Blockchain size as 500, Genuine user detection rate

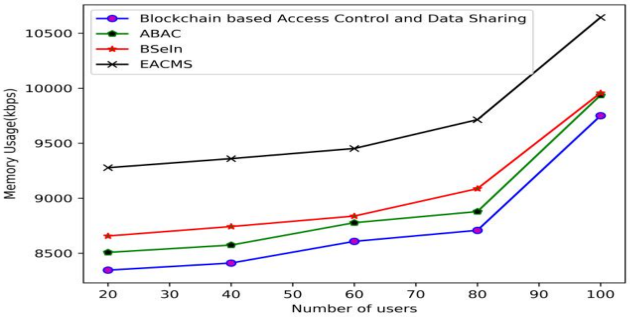

Figure 6 b) Comparative analysis with the Blockchain size as 500, Memory usage

4.5 Comparative discussion

Table 1 represents the relative discussion. Using the Blockchain size of 100, the Genuine user detection rate found by the present approaches, like ABAC, BSeIn, and EACMS is 65%, 65%, and 58%, whereas the projected found enhanced Genuine user detection rate of 95%, correspondingly. The Memory usage obtained is the existing methods, such as ABAC, BSeln and EACMS is 4950.63kbps, 4980.77kbps, and 5303.02kbps, whereas the proposed obtained lower memory usage of 4837.99 for the block size 300. So, it is noticeably represented that the projected approach achieved improved genuine user detection rate of 95%, and lower memory usage of 1580 kbps using the Blockchain size as 100, respectively.

Table 1: Comparative discussion

Blockchain size	**Metrics**	**ABAC**	**BSeIn**	**EACMS**	**Proposed Blockchain-based access control and data sharing**
100	Genuine user detection rate (%)	65	65	58	95
	Memory usage (kbps)	1620	1730	1730	1580
200	Genuine user detection rate (%)	83	70	38	95
	Memory usage(kbps)	3414.88	3504.83	3648.87	3347.84
300	Genuine user detection rate (%)	75	69	68	95
	Memory usage(kbps)	4950.63	4980.77	5303.02	4837.99
400	Genuine user detection rate (%)	83	83	61	95
	Memory usage (kbps)	5888.01	5757.48	6332.93	5620.57
500	Genuine user detection rate (%)	61	57	49	95
	Memory usage(kbps)	8507.45	8656.83	9277.58	8346.04

5. CONCLUSION

In this article, we projected innovative authentication centered access mechanism and data sharing system in cloud centered on Blockchain. Blockchain technology remains foremost opportunity used for making safe data as well as secrecy of users in cloud. The rise of the blockchain has permitted us to attach by storing space, bandwidth, CPU power, etc. This decentralized and Blockchain based access control scheme will resolve the problematic lack of trust and prepared the system extra robust. The proposed named Blockchain-based access control and data sharing methodology achieved superior performance with the metrics, such as better Genuine user detection rate of 95% and Memory usage of 1580 kbps through the Blockchain of 100 size. In forthcoming, the performance of the access control in addition data sharing prototypical inside the cloud storing scheme is improved via integrating certain extra features.

REFERENCES

1. Rajput, A.R., Li, Q., Ahvanooey, M.T. and Masood, I., "EACMS: Emergency Access Control Management System for Personal Health Record based on Blockchain", IEEE Access. 2019.
2. Ding, S., Cao, J., Li, C., Fan, K. and Li, H., "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT", IEEE Access, vol. 7, pp.38431-38441, 2019.
3. Ma, M., Shi, G. and Li, F., "Privacy-Oriented Blockchain-based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario", IEEE Access, vol. 7, pp.34045-34059, 2019.
4. Ouaddah, A., Elkalam, A.A. and Ouahman, A.A., "Towards a novel privacy-preserving access control model based on blockchain technology in IoT", In Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523-533, Springer, Cham, 2017.
5. Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H. and Ali, Q.E., "Blockchain based Permission Delegation and Access Control in Internet of Things (BACI)", Computers & Security, 2019.
6. Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B., "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustainable Cities and Society, vol. 39, pp.283-297, 2018.
7. Lin, C., He, D., Huang, X., Choo, K.K.R. and Vasilakos, A.V., "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0", Journal of Network and Computer Applications, vol. 116, pp.42-52, 2018.
8. Wang, S., Zhang, Y. and Zhang, Y., "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems", IEEE Access, vol. 6, pp.38437-38450, 2018.
9. Benchoufi, M. and Ravaud, P., "Blockchain technology for improving clinical research quality", Trials, vol. 18, no. 1, p.335, 2017.
10. Es-Samaali, H., Outchakoucht, A. and Leroy, J.P., "A blockchain-based access control for big data", International Journal of Computer Networks and Communications Security, vol. 5, no. 7, p.137, 2017.
11. Iansiti, M. and Lakhani, K.R., "The truth about blockchain", Harvard Business Review, vol. 95, no. 1, pp.118-127, 2017.
12. Zyskind, G. and Nathan, O., "Decentralizing privacy: Using blockchain to protect personal data", IEEE Security and Privacy Workshops, pp. 180-184, May 2015.
13. Rahulamathavan, Y., Phan, R.C.W., Rajarajan, M., Misra, S. and Kondoz, A., "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption", IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, December 2017.
14. JKR Sastry, B. TrinathBasu, "Implementing User defined Attribute and Policy based Access Control", International Journal of Emerging Trends in Engineering Research, Volume 8. No. 7, July 2020,
15. Tatyana Deeva1, Galina Nikiporets-Takigawa, " Blockchain Technologies and Smart Contracts: New Technological Methods to Regulate Transactions and Trade Operations", International Journal of Emerging Trends in Engineering Research, Volume 8. No. 7, July 2020.