ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

ENABLING TRUST AND PRIVACY- PRESERVING e-KYC SYSTEM USING BLOCKCHAIN

Mohd Mudabbir Ahmed Furqan[1], Subramanian K.M [2], Imtiyaz Khan[3]

[1]PG Scholar, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.
furqanmudabbir@gmail.com.

[2]Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.
kmsubbu.phd@gmail.com

[3]Professor, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.
imtiyaz.khan.7@gmail.com

ABSTRACT

The electronic know your client (e-KYC) is a framework for the banking or personality supplier to lay out a client character information check process between depending parties. Because of the proficient asset utilization and the serious level of openness and accessibility of distributed computing, most banks carry out their e-KYC framework on the cloud. Basically, the security and protection of e-KYC related reports put away in the cloud turns into the urgent issue. Existing e-KYC stages for the most part depend areas of strength for on and apply customary encryption to help their security and protection necessity. In this model, the KYC framework proprietor scrambles the document with their host's critical and transfers it to the cloud. This technique initiates encryption reliance and correspondence and key administration overheads. In this paper, we present a clever block chain-based e-KYC plot called e-KYC Trust Block in view of the ciphertext strategy characteristic based encryption (CP-ABE) technique restricting with the client agree requirement to convey trust, security and protection consistence. What's more, we acquaint property based encryption with empower the security protecting and fine-grained admittance of touchy exchanges put away in the block chain. At last, we direct tests to show that our framework is effective and versatile by and by.

INTRODUCTION

Electronic-Know your client (e-KYC) is a help that banks or monetary foundations (FIs) give virtual financial activity connected with validation and check of personality electronically to their clients for working on cost proficiency and consumer loyalty. The e-KYC framework empowers FIs to electronically confirm their client personality and recover KYC information for both individual and corporate clients. To carry out the e-KYC framework, monetary foundations either utilize off the-rack e-KYC programming completely furnished with vital capabilities or create their own. Then, they can send the framework as an on premise or a cloud-based model. Because of the pattern of the re-appropriating model, most endeavors have embraced the cloud as the favored stage for lodging their framework and information. A cloud-based e-KYC framework gives a more proficient and adaptable confirmation technique contrasted with the host based e-KYC verification strategy where reports should be approved by means of the incorporated host. This causes a traffic bottleneck and weak link issue. Additionally, the recognizability of the checked exchange is restricted since all exchanges happening in the framework are totally overseen by the supplier.

By and by, the security and protection issue of a cloud-based arrangement is a worry for the vast majority possible endeavors. This is on the grounds that e-KYC framework situated on the cloud store client information reports and it very well may be seen by any open cloud occupants or even the cloud specialist co-ops (CSPs). To address this worry, most banks and FIs need to carry out an encryption component notwithstanding the solid confirmation include given by the CSPs.

To this end, banks and FIs having the e-KYC framework need to scramble the e-KYC information records before they are transferred to the cloud. While

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

the depending parties demand for check, the host party can either play out the confirmation by either unscrambling the record and sending back the affirmation of the check result to the requestor or communicating the duplicate of encoded documents alongside the decoding key to the requestor. This first methodology acquaints the overheads related with the confirmation cycle, correspondence, and unified unscrambling while the last option approach requirements to deal with key administration particularly secure key sharing. In particular, key disavowal and key re-age in the cloud e-KYC climate have not been tended to by any exploration works. Assuming the client might want to pull out his assent from any banks or FIs, they reserve no option to store the client's personality information any longer. Likewise, the information ought to be totally erased and the unscrambling key should be renounced. Any banks or FIs sharing the disavowed key need to recover a key to completely ensure that unapproved banks or FIs can't get to the client's information put away in the cloud. Notwithstanding the previously mentioned issues, leaving cloud e-KYC stages don't give shared data to the exchange happening in the e-KYC check accessible for detectability. As of late, block chain innovation has drawn in gigantic premium by various undertakings in numerous enterprises including the banking and monetary area.

There is a developing interest in utilizing e-KYC stages that utilization block chain and cloud framework. Block chain innovation genuinely advances the decentralized framework empowering straightforwardness, readiness, reliability, and cost-adequacy for exchange handling and the board in multi-client and multi-supplier climate. In the block chain framework, a savvy contract which is a self-executing program that can be carried out on the block chain empowers the robotized execution of framework rationales or works proficiently. This enables the convenience and programmability of any frameworks running on the blockchain network. For quite a long time, various examination works connected with blockchain-based KYC have proposed to convey the decentralized validation and confirmation process. Nonetheless, there are inadequacies that poor person been completely settled by existing works. In the first place, there are no works that furnish electronic client's assent capability with the strong nonrepudiation property which is a fundamental prerequisite of security guidelines, for example, General Information Assurance Act (GDPR) [18] in the KYC enlistment process. Second, most existing works disregard the security of exchange put away in the brilliant agreement and blockchain. Notwithstanding the character or certification reports that are scrambled on the distributed storage, the protection of all e-KYC handling exchanges, for example, exchange status sharing, information beginning verification, and savvy contract that contains individual information put away in the blockchain ought to be safeguarded. At long last, most works have a restricted element to permit the clients to access and refresh their certifications situated on the cloud administration paid by the FI. In this paper, we mean to address such examination holes by presenting a solid and effective blockchain-based eKYC reports enrollment and check process with lightweight key cryptographic conventions run in the cloud Interplanetary Document Framework (IPFS). To work with the primary protection prerequisite in regards to the client's assent assortment, we foster a shrewd agreement to produce and uphold the agree to be carefully endorsed by the client. The assents will be efficiently put away in a blockchain having carefully designed property which is valuable for examining.

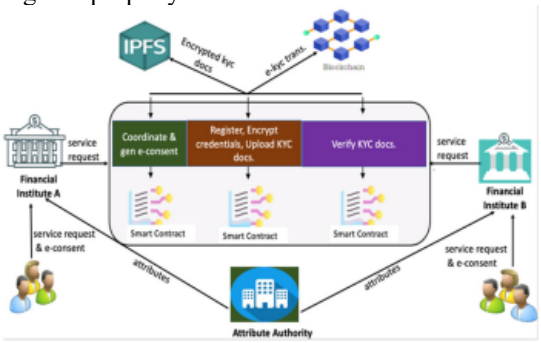


Fig 1: Block Diagram of Sharing Moment

Technologies that effectively safeguard data in a shared environment. For numerous applications, a variety of approaches for data protection in the cloud environment have been investigated and developed. This article focuses on providing effective protection by avoiding leakage and identifying the malevolent entity responsible for leakage as shown in Fig. 2. Typically, data protection is performed by leakage prevention and leaker detection. The primary strategies for preventing data leakage are customized using machine learning techniques, access control systems, differential privacy, and cryptography, whereas the main methods for detecting leakers include watermarking and probabilistic methods.

MOTIVATION

At present, blockchain technology and smart contracts have been leveraged in many application areas. Particularly, blockchain-based identification and authentication framework have been proposed by many works and it has been demonstrated that a blockchain is efficient for identification and authentication

management. However, the process of e-KYC is much more complicated than simple authentication task. Rather, it involves secure credential registration, KYC document management, secure and lightweight verification process between clients, multiple FIs, and a dedicated blockchain platform. In addition, new kinds of remote and spoofing attack to the KYC system need to be countered. Recent research works related to a blockchain-based e-KYC focus on devising a framework for secure user identity management and credentials verification as well as optimizing the communication overhead of the interaction among financial institutes. In [3], the authors proposed a KYC document verification scheme using the IPFS system and blockchain technology. In this approach, the customers register their identity information with the bank and their credentials are hashed and encrypted by using gpg4win as an encryption tool. However, this paper does not concern itself with the privacy and traceability of transactions in the block chains. In [5], Shabair et al. proposed a blockchain-based KYC in the form of proof-of-concept (PoC) system. The proposed system was conducted in private blockchain environments over the Grid'5000 a large-scale distributed platform.

OUR CONTRIBUTION

The following is a summary of the article's significant contributions:

1) The main and important methods for data security through safe sharing in a cloud context are reviewed in this paper.

2) We offer the following information regarding each strategy.

(a)How it functions in terms of data protection, and (b) the superior, ground-breaking options available.

In order to make it simple for readers to understand the essence of the approach as well as its applications, we also include potential and valuable information about each presented solution in a tabular manner, such as its working, implementation environment, success, range of the provided model, etc.

3) A thorough and comparative study of the methodologies covered is conducted and presented in an accessible manner. Additionally, research is done to determine which technique will best meet the needs.

EXISTING SYSTEM:

For years, a number of research works related to block chain-based KYC have proposed to deliver the decentralized authentication and verification process. However, there are shortcomings that have not been fully solved by existing works. First, there are no works that provide electronic client's consent function with the solid non repudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and blockchain. In addition to the identity or credential documents that are encrypted on the cloud storage, the privacy of all e-KYC processing transactions such as transaction status sharing, data origin authentication, and smart contract that contains personal data stored in the blockchain should be preserved.

Existing System Disadvantages:

- Decentralized authentication.
- Verification process.

LITERATURE SURVEY

Distributed blockchain-based authentication and authorization protocol for smart grid.

Authentication and authorization (A & A) mechanisms are critical to the security of Internet of Things (IoT) applications. Smart grid system processing and exchanging data without human intervention, known as smart grids, are well-known as IoT scenarios. Entities in such smart grid systems need to identify and validate one another and ensure the integrity of data exchange mechanisms. However, at present, most commonly used A & A protocols are centralized, resulting in security risks such as information leaks, illegal access, and identity theft. In this study, we propose a new distributed A & A protocol for smart grid networks based on blockchain technology to address with these risks. The proposed protocol integrates the decentralized authentication and immutable ledger characteristics of blockchain architectures suitable for power systems with a novel blockchain technique to realize both identity authentication and resource authorization for smart grid systems. We discuss the security of and threat models for prior A & A protocols and demonstrate how our protocol protects against these threats. We further demonstrate an approach to a real deployment of our A & A protocol using the FISCO consortium platform, applying algorithms from smart contract systems. Finally, we present the results of experimental simulations showing the efficacy and efficiency of our proposed protocol.

Blockchain technology the identity management and authentication service disruptor: A survey.

The Internet today lacks an identity protocol for identifying people and organizations. As a result, service providers needed to build and maintain their own databases of user information. This solution is costly to the service providers, inefficient as much of

the information is duplicated across different providers, difficult to secure as evidenced by recent large-scale personal data breaches around the world, and cumbersome to the users who need to remember different sets of credentials for different services. Furthermore, personal information could be collected for data mining, profiling and exploitation without users' knowledge or consent. The ideal solution would be self-sovereign identity, a new form of identity management that is owned and controlled entirely by each individual user. This solution would include the individual's consolidated digital identity as well as their set of verified attributes that have been cryptographically signed by various trusted issuers. The individual provides proof of identity and membership by sharing relevant parts of their identity with the service providers. Consent for access may also be revoked hence giving the individual full control over its own data. This survey critically investigates different blockchain based identity management and authentication frameworks. A summary of the state-of-the-art blockchain based identity management and authentication solutions from year 2014 to 2018 is presented. The paper concludes with the open issues, main challenges and directions highlighted for future work in this area. In a nutshell, the discovery of this new mechanism disrupted the existing identity management and authentication solutions and by providing a more promising secure platform.

Secure and transparent KYC for banking system using IPFS and blockchain technology.

With continuously changing operational and business needs of the organizations, Decentralized Autonomous Organizations (DAO) is the current need of the organizations. Centralized Autonomous Organization (CAO) lack transparency and are managed by few efficient managers whereas Decentralized autonomous Organization's (DAO) is novel scalable, self-organizing coordination on the blockchain, controlled by smart contracts and its essential operations are automated agreeing to rules and principles assigned in code without human involvement. In this chapter we discuss the needs for Decentralized Autonomous Organizations (DAO) and key efforts in this field. We then introduce a prospective solution employing block chain Ethereum, which incorporates a Turing complete programming language with smart contract computing functionality. A solution is elaborated that permits the formation of organizations where participants preserve straight real-time check of contributed collects and governance policies are formalized, automatized and imposed using software. Basic code for smart contract is composed to make a Decentralized Autonomous Organization (DAO) on the Ethereum block chain. We also explain the working of DAOs code, centering on fundamental establishment and governance characteristics, which includes organization, formation and voting rights. DAOs are considered to agree to the expectation of the business work in the future. But there is still lack of operational base for DAOs in the blockchain community.

Blockchain orchestration and experimentation framework: A case study of KYC.

Conducting experiments to evaluate blockchain applications is a challenging task for developers, because there is a range of configuration parameters that control blockchain environment. Many public testnets (e.g. Rinkeby Ethereum) can be used for testing, however, we cannot adjust their parameters (e.g. Gas limit, Mining difficulty) to further the understanding of the application in question and of the employed blockchain. This paper proposes an easy-to-use orchestration framework over the Grid'5000 platform. Grid'5000 is a highly reconfigurable and controllable large-scale testbed. We developed a tool that facilitates nodes reservation, deployment and blockchain configuration over the Grid'5000 platform. In addition, our tool can fine-tune blockchain and network parameters before and between experiments. The proposed framework offers insights for private and consortium blockchain developers to identify performance bottlenecks and to assess the behavior of their applications in different circumstances.

Identity and access management with blockchain in electronic healthcare records.

Blockchain has proved itself to be tamper resistant and secure. It is increasingly getting attention from companies changing from centralized to decentralized systems. This paper proposes a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system. A prototype demonstrates the application of blockchain in identity and access management using the hyper ledger Fabric framework. It provides a proof of concept based on a use case concerning Electronic Health Records from the healthcare domain where an immutable and auditable history is desired for data concerning patients. Basic authentication and authorization operations are able to execute in 2-3 seconds with an initial size of blockchain of about 3.8 MB covering physicians in Denmark.

PROPOSED SYSTEM

According to this paradigm, the file is encrypted using the host's key and uploaded to the

cloud by the owner of the KYC system. This approach results in communication, key management, and encryption dependence overheads. In this work, we provide e-KYC Trust Block, a unique blockchain-based e-KYC scheme that binds client consent enforcement with cypher text policy attribute-based encryption (CP-ABE) method binding to deliver trust, security, and privacy compliance. Additionally, we propose attribute-based encryption to make it possible for sensitive transactions stored on the blockchain to be accessed with great precision while maintaining privacy. Finally, we run tests to demonstrate the practical scalability and efficiency of our system.

ADVANTAGE

- Attribute-based encryption to enable the privacy preserving.
- Induces encryption dependency and communication.
- Key management overheads.

MODULES NAME

1. Authority

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. Clients

This is the second module Data User can register and Login. After login Data User have an option of searching the files as a file name. Data user can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the request and then data user can takes permissions from the owner then the file it will downloaded in plain text.

3. Users

This is the third module of this project. In this module Data Owner should register and Login. Data Owner will Uploads the files into the database. Data owner can also send request to the data user.

PROPOSED ALGORITHM

- **CP-ABE with Blockchain algorithm**

Proposed a traceable attribute-based encryption with dynamic access control (TABE-DAC) scheme based on the combination of CP-ABE based linear secret sharing scheme (LSSS) and blockchain. The proposed scheme achieves fine-grained sharing of encrypted private data on cloud, traceability of users' private key leakage, and flexible policy update. The authors also introduced a hash function in the key and ciphertext generation to reduce the computation cost of such operations. In these schemes, any changes to the data are recorded on the blockchain and the access policy is enforced to manage the different permissions of access. If there is any key abuse case initiated by any malicious users or authorities, the system provides audit trails to support the traceability of cryptographic operations and transaction activities.

Regarding the data privacy issue, we propose an optimized cryptographic protocol by applying symmetric encryption with public key encryption to encrypt the customers' credential files and employ the ciphertext policy attribute-based encryption (CP-ABE) to encrypt the blockchain transactions. Since CP-ABE provides a one-to-many encryption with fine-grained access control, it allows several FIs to access common encrypted transactional data in the blockchain of the same client based on the access policy defined. Specifically,

we devise the policy update algorithm to enable efficient re-encryption based on a less complicated policy tree structure. Finally, our system allows users to update their e-KYC data with any banks or FIs engaging in the blockchain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract.

EXISTING ALGORITHM

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

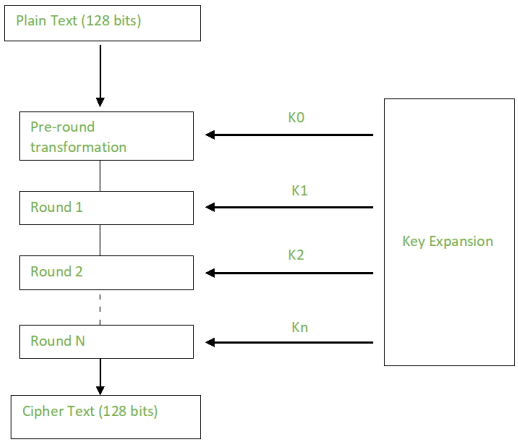
That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024



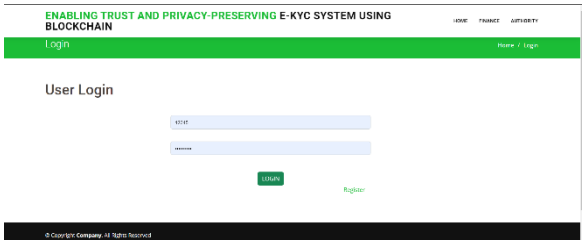
The number of rounds depends on the key length as follows:

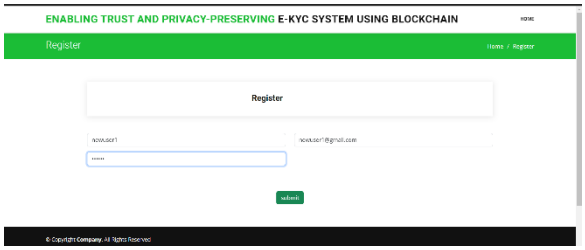
- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

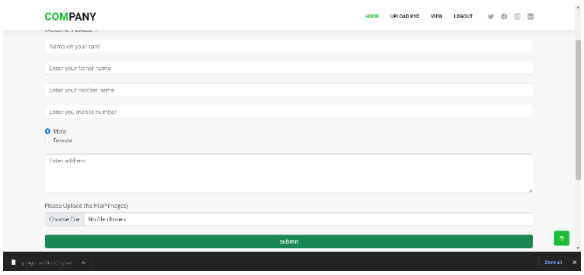
Creation of Round keys:

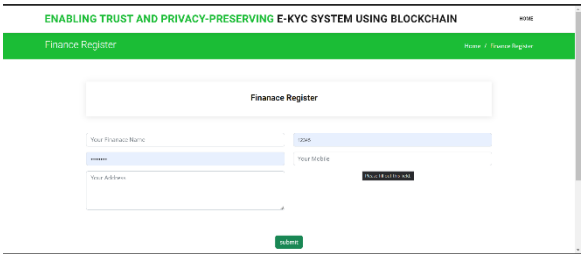
A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

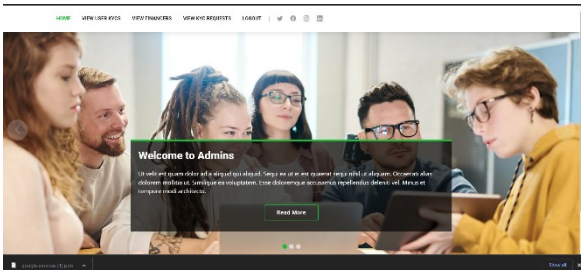
SCREENSHOTS











FUTURE ENHANCEMENT

For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the blockchain with the searchable encryption feature.

CONCLUSION

We have presented the privacy-preserving e-KYC approach based on the blockchain. Our proposed scheme delivers secure and decentralized authentication

and verification of the e-KYC process with the user's consent enforcement feature. In our scheme, the privacy of both customers' identity documents stored in the cloud is guaranteed by the symmetric key and public key encryption while the sensitive transaction data stored in the blockchain is encrypted by symmetric key encryption and CP-ABE. Our scheme also allows the KYC data to be updated by the data owner or the customer. In addition, we devised an access policy update algorithm to enable dynamic access authorization. For the evaluation, we performed comparative analysis between our scheme and related works in terms of the computation cost, the communication cost, and performance. The experimental results showed that our scheme outperforms existing schemes in terms of performance, comprehensive KYC compliance features, and the scalable access control mechanism. For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the blockchain with the searchable encryption feature.

REFERENCES

[1] A. K. Singh and I. Gupta, ``Online information leaker identification scheme for secure data sharing," Multimedia Tools Appl., vol. 79, no. 41, pp. 31165_31182, Nov. 2020.
[2] E. Zaghloul, K. Zhou, and J. Ren, ``P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing," IEEE Trans. Big Data, vol. 6, no. 4, pp. 804_815, Dec. 2020.
[3] I. Gupta and A. K. Singh, ``GUIM-SMD: Guilty user identification model using summation matrix-based distribution," IET Inf. Secur., vol. 14, no. 6, pp. 773_782, Nov. 2020.
[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331_346, Feb. 2019.
[5] I. Gupta and A. K. Singh, ``an integrated approach for data leaker detection in cloud environment," J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993_1005, Sep. 2020.
[6] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ``A lightweight secure data sharing scheme for mobile cloud computing," IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344_357, Apr. 2018.
[7] I. Gupta, N. Singh, and A. K. Singh, ``Layer-based privacy and security architecture for cloud data sharing," J. Commun. Softw. Syst., vol. 15, no. 2, pp. 173_185, Apr. 2019.
[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ``an efficient attribute-based encryption scheme with policy update and update in cloud computing," IEEE Trans. Ind. Informant., vol. 15, no. 12, pp. 6500_6509, Dec. 2019.
[9] C. Suisse. (2017). 2018 Data Center Market Drivers: Enablers Boosting Enterprise Cloud Growth. Accessed: May 19, 2019. [Online]. Available: https://cloudscene.com/news/2017/12/2018-data-center-predictions/
[10] I. Gupta and A. K. Singh, ``A framework for malicious agent detection in cloud computing environment," Int. J. Adv. Sci. Technol., vol. 135, pp. 49_62, Feb. 2020.
[11] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, ``Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Trans. Dependable Secure Comput., vol. 16, no. 1, pp. 72_83, Jan. /Feb. 2019.
[12] I. Gupta and A. K. Singh, ``A probabilistic approach for guilty agent detection using bigraph after distribution of sample data," Proc. Comput. Sci., vol. 125, pp. 662_668, Jan. 2018.
[13] L. Zhang, Y. Cui, and Y. Mu, ``Improving security and privacy attribute based data sharing in cloud computing," IEEE Syst. J., vol. 14, no. 1, pp. 387_397, Mar. 2020.
[14] I. Gupta and A. K. Singh, ``Dynamic threshold based information leaker identification scheme," Inf. Process. Lett., vol. 147, pp. 69_73, Jul. 2019.
[15] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, ``An efficient _le hierarchy attribute-based encryption scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265_1277, Jun. 2016.
[16] I. Gupta and A. K. Singh, ``SELI: Statistical evaluation based leaker identification stochastic scheme for secure data sharing," IET Commun., vol. 14, no. 20, pp. 3607_3618, Dec. 2020.
[17] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, ``Attribute-based access control with constant-size ciphertext in cloud computing," IEEE Trans. Cloud Comput., vol. 5, no. 4, pp. 617_627, Oct./Dec. 2017.
[18] I. Gupta and A. K. Singh, ``A probability based model for data leakage detection using bigraph," in Proc. 7th Int. Conf. Commun. Netw. Secure. (ICCNS). New York, NY, USA: Assoc. Comput. Machinery, 2017, pp. 1_5.
[19] L. Columbus. (Jan. 2018). 83% of Enterprise Workloads Will Be in the Cloud by 2020. [Online]. Available workloads-will-be-in-the-cloud-by-2020/#50d375286261

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

[20] Gartner. (2018). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. [Online]. Available: gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percentin- 2019
[21] (2019). Cloud IT Infrastructure Revenues Surpassed Traditional IT Infrastructure Revenues for the First Time in the Third Quarter of 2018. Accessed: May 19, 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS44670519
[22] (Dec. 2021). Alarming Cyber Security Facts to Know for 2021 and Beyond. [Online]. Available: security-facts-to-know-for-2021-and-beyond/
[23] W. Li, K. Xue, Y. Xue, and J. Hong, ``TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 5, pp. 1484_1496, May 2016.
[24] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, ``PDLM: Privacy-preserving deep learning model on cloud with multiple keys," IEEE Trans. Services Comput., vol. 14, no. 4, pp. 1251_1263, Jul. 2021.
[25] I. Gupta and A. K. Singh, ``A confidentiality preserving data leaker detection model for secure sharing of cloud data using integrated techniques," in Proc. 7th Int. Conf. Smart Compute. Communication (ICSCC). Sarawak, Malaysia: Curtin Univ., Jun. 2019, pp. 1_5.