Signature-Based Public Sensitive Data Sharing for Cloud Storage

Kanchana A[1], Sriram R[2*], Rithik M R[3], VijayVikraman V[4z]

akanchana2683@gmail.com [1], Assistant Professor, Department of Computer Science and Engineering, Panimalar Engineering College [Autonomous],Tamil Nadu, India

sriramrajendran74@gmail.com, rithikmr17@gmail.com, vijayvik28@gmail.com-[2,3,4] ,Department of Computer Science and Engineering, Panimalar EngineeringCollege [Autonomous], Tamil Nadu, India

Abstract: To ensure information security, the information proprietor necessities to check the respectability of information put away somewhat in the cloud server with the public examining method. In reality the staff needs to enlist here and it will tell to the group chief who needs to support to their worker. In the future who can login in this application in light of group like A, B, C, D. The group can share the venture subtleties to a workers. In the event that the subtleties added by Group A representative's, it will tell to Group A worker's not to other people. Before that the group chief added by the administration and keep up with the group chief's subtleties. The staff could ready to see the encoded subtleties just not the first happy it will be changed over completely to cryptography design. Cryptography is procedure of getting data and correspondences through utilization of codes with the goal that main those individual for whom the data is planned can grasp it and interaction it. The solicitation of staffs move to the group chief who needs to support it then, at that point, moved to the administration who will check staff subtleties and group pioneers. After the endorsement the staff can recover the information utilizing the QR. A QR code is a sort of standardized identification that can be perused effectively by a computerized gadget and which stores data as a progression of pixels in a square-formed matrix

1.Introduction

This application presents an execution for data splitting between applications considering hilter kilter encryption computations, high level mark. It in like manner gives a momentous idea of data splitting between applications. Today, dispersed capacity becomes one of the fundamental organizations, since clients can without a doubt change and proposition data with others in cloud. Nevertheless, the genuineness of shared cloud data is helpless against unpreventable gear imperfections, programming dissatisfactions or human bumbles. To ensure the uprightness of the normal data, a couple of plans have been expected to allow public verifiers (i.e., untouchable commentators) to survey data decency without recuperating the entire clients' data from cloud beneficially. Unfortunately, public looking at on the reliability of shared data could reveal data owners' fragile information to the pariah evaluator. In this paper, we propose one more insurance careful public surveying part for shared cloud data by building a homomorphic verifiable get-together imprint.) the result of secure computation prohibits 0. Inconsistent numbers revamped by each server are fixed and each server holds unpredictable numbers dark to the adversary and holds parts of sporadic numbers that make up the unpredictable numbers dark to the foe. Secret sharing is a critical means to achieve characterization and data security. Secret contribution game plans to separating a limited information with various players. The target of the secret sharing is security of secret, insurance and disguising information. This application will stay aware of the strong data move with individual social affair bunch trailblazers and delegates then organization will support for data sharing. This application will run in various administrative groups.

1.1Database

In computing, a database is an organized collection of data stored and accessed electronically. Small databases can be stored on a file system, while large databases are hosted on computer clusters or cloud storage. The design of databases spans formal techniques and practical considerations, including data modeling, efficient data representation and storage, query languages, security and privacy of sensitive data, and distributed computing issues, including supporting concurrent access and fault tolerance. A database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the database. The sum total of the database, the DBMS and the associated applications can be referred to as a database system. Often the term "database" is also used loosely to refer to any of the DBMS, the database system or an application associated with the database. Computer scientists may classify database management systems according to the database models that they support. Relational databases became

dominant in the 1980s. These model data as rows and columns in a series of tables, and the vast majority use SQL for writing and querying data. In the 2000s, non-relational databases became popular, collectively referred to as NoSQL, because they use different query languages.

1.2AES Algorithm

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The AES algorithm is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0. NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits.

- Security. Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.

- Cost. Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

- Implementation. Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

Encryption In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. For technical reasons, an encryption scheme usually uses a pseudorandom encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Decryption The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

1.3Modules

The register module provides a conceptual framework for entering data on those staff in a way that: eases data entry & accuracy by matching the staff entry to the data source (usually paper files created at point of care), ties easily back to individual staff records to connect registers to staff data, and collects data elements to enable better supervision of donation programs. here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. the staff will also view the team leader added file. And analysis the details will be responsible for your file stored in database.

2.Literature Survey

1.TITLE: Research of Data Sharing between Applications Base on User Request AUTHOR: Xie Suping, Chen Huaichu, Luo Nianlong, Zhang Huilin YEAR: 2015 **PAPER EXPLANATION** This paper presents an implementation for data sharing between applications based on asymmetric encryption algorithms, digital signature. It also provides a new idea of data sharing between applications. It can be a supplementary program for data sharing. It can be an effective solution to solve the problem of sensitive personal data grant between applications data and can be used for proof of personal income data, statistical data sharing and the like.

2.TITLE: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users AUTHOR: Anmin Fu; Shui Yu; Yuqing Zhang; Huaqun Wang; Chanying Huang YEAR: 2017 **PAPER EXPLANATION** Today, cloud storage becomes one of the critical services, because users can easily modify and share data with others in cloud. However, the integrity of shared cloud data is vulnerable to inevitable hardware faults, software failures or human errors. To ensure the integrity of the shared data, some schemes have been designed to allow public verifiers (i.e., third party auditors) to efficiently audit data integrity without retrieving the entire users' data from cloud. Unfortunately, public auditing on the integrity of shared data may reveal data owners' sensitive information to the third party auditor. In this paper, we propose a new privacyaware public auditing mechanism for

shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least t group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides nonframeability. Moreover, our scheme ensures that group users can trace data changes through designated binary tree; and can recover the latest correct data block when the current data block is damaged. In addition, the formal security analysis and experimental results indicate that our scheme is provably secure and efficient.

3.TITLE: Secure Computation by Secret Sharing using Input Encrypted with Random Number. AUTHOR: Keiic Keiichi Iwamura and Ahmad Akmal Aminuddin Mohd Kamalhi Iwamura and Ahmad Akmal Aminuddin Mohd Kamal YEAR: 2019 **PAPER EXPLANATION** Typically, unconditionally secure computation using a (k, n) threshold secret sharing is considered impossible when $n < 2k - 1$. Therefore, in our previous work, we first took the approach of finding the conditions required for secure computation under the setting of $n < 2k - 1$ and showed that secure computation using a (k, n) threshold secret sharing can be realized with a semihonest adversary under the following three preconditions: (1) the result of secure computation does not include 0; (2) random numbers reconstructed by each server are fixed; and (3) each server holds random numbers unknown to the adversary and holds shares of random numbers that make up the random numbers unknown to the adversary. In this paper, we show that by leaving condition (3), secure computation with information-theoretic security against a semi-honest adversary is possible with $k \leq n < 2k - 1$. In addition, we clarify the advantage of using secret information that has been encrypted with a random number as input to secure computation. One of the advantages is the acceleration of the computation time. Namely, we divide the computation process into a preprocessing phase and an online phase and shift the cost of communication to the preprocessing phase. Thus, for computations such as inner product operations, we realize a faster online phase, compared with conventional methods.

4.TITLE: Secure Secret Sharing Using Homomorphic Encryption AUTHOR: Nileshkumar Kakade; Utpalkumar Patel YEAR: 2020 **PAPER EXPLANATION** Secret sharing is an important means to achieve confidentiality and data privacy. Secret sharing deals with splitting a secret information with various players. The goal of the secret sharing is security of secret, privacy and hiding information. There are numerous techniques available for secret sharing e.g. polynomial, Chinese remainder theorem, vector space, matrix projection. Techniques have characteristics like threshold, proactive, verifiable. Proactive secret sharing scheme allow user to change share in case of doubt of theft. In this work we propose the proactive secret sharing scheme based on homomorphic techniques. Our scheme consists of three phases of share construction, share renewal, share reconstruction. Central authority splits an encrypted secret with each parties using homomorphic property of paillier encryption i.e. subtraction. In renewal process two or more parties relate share with each other for to generated renewed share. In reconstruction process all parties share will be add to central authority then encrypted secret will be generated. Central authority will decrypt encrypted secret using secret key then original secret will be generated. Our schemes unique features is share can be renewed any time, Each party can choose secret of their own choice, If any two parties have same content share then also encrypted share will be different due to non-deterministic property of paillier encryption.

5.TITLE: Secure multi-party computation in differential private data with Data Integrity Protection AUTHOR: Sundari S, Ananthi M YEAR: 2015 **PAPER EXPLANATION** Secure multiparty computation (SMC) is needed now-a-days in which data are distributed between different parties. Moreover, organizations are wished to collaborate with other parties who conduct same business, for their mutual benefits. SMC provides users to gain much information from the larger data without disclosing the data. This project combines the technique secure multiparty computation and the differential privacy for vertically partitioned data between parties. To achieve this, a multi-party protocol has been proposed for the exponential mechanism. Reliable access to data is must for most computer applications and data servers. Some factors causes unauthorized access to stored data. Two Phase Validation (2PV) provides the authentication for the users, while integrating the data in multiparty computation. Data can get corrupted due to some malfunctions. Disk errors are common today but the storage technologies are not designed to handle such kind of errors. A simple integrity violation is detected by the higher level software which causes further loss of data. The proposed system is to verify the integrity of random subsets of data against general or malicious corruptions through Distributed Data Integrity (DDI) Protection.

3.Existing System

A public auditing scheme that supports sensitive data sharing for the cloud environment. In our scheme, the data owner's privacy can be protected while sharing data. The integrity checking of the remotely stored data in the cloud server can also be executed efficiently. The security analysis shows that our proposed scheme is more secure compared to that of related works, and several experiments show that our scheme achieves a desirable efficiency.

Technique: Bilinear pairing and cryptographic difficult problems

Disadvantages:It takes a long time to process function methods.

4.Proposed System

We propose another plan in light of the redactable signature. In our proposed plot, the cloud server can change the mark straightforwardly without the extra sanitizer while sharing delicate information.

Technique: RSA algorithm. SQL Operation

Advantages: It gives a standard and valid solution to process the data with has to function.

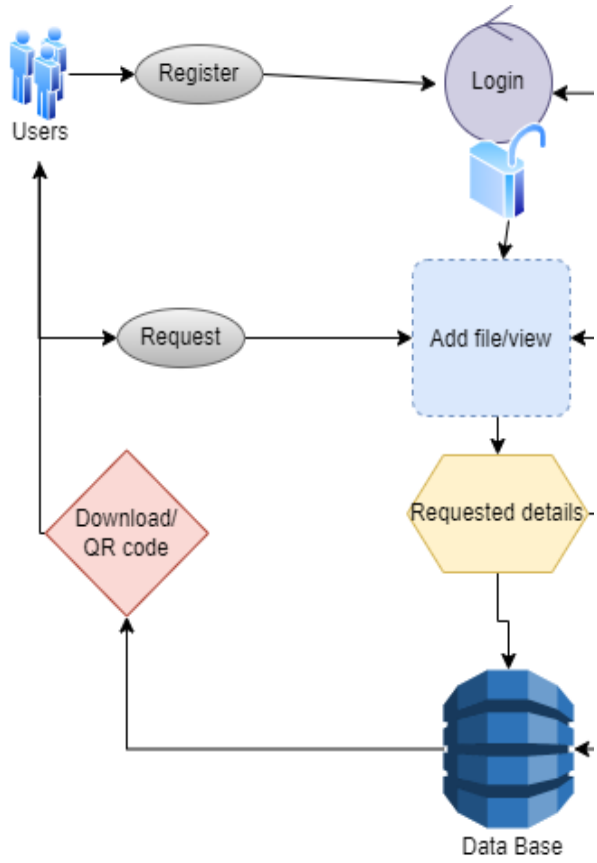

Fig. 1 – Architecture diagram of the proposed system

5.Conclusion

Data sensitivity concerns information that should be protected from unauthorized access or disclosure due to its sensitive nature. For some, that might be Team leader, Staff details records. Sensitive data is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent.

6.References

[1] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, vol. 6, no. 2, pp. 147-156, 2020.

[2] D. Liu and J. Lee, "CNN based Malicious Website Detection by Invalidating Multiple Web Spams," IEEE Access, vol. 8, no. 1, pp. 97258-97266, 2020.

[3] W. Martin, V. Friedhelm, and K. Axel, "Tracing manufacturing processes using blockchain-based token compositions," Digital Communications and Networks, vol. 6, no 2, pp. 167-176, 2019.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, 2018.

[5] L. Peng, W. Feng, and Z. Yan. (2020). Privacy preservation in permissionless blockchain: A survey. Digital Communications and Networks. [Online]. Available: https://doi.org/10.1016/j.dcan.2020.05.008.

[6] N. Kakade and U. Patel, "Secure Secret Sharing Using Homomorphic Encryption," in Proc. 2020 11th International Conference on Computing, Communication and Networking Technologies, 2020, pp. 1-7.

[7] S. Sundari and M. Ananthi, "Secure multi-party computation in differential private data with Data Integrity Protection," in Proc. 2015 International Conference on Computing and Communications Technologies, 2015, pp. 180- 184.

[8] S. Jiao, T. Lei, Y. Gao, Z. Xie and X. Yuan, "Known-Plaintext Attack and Ciphertext-Only Attack for Encrypted Single-Pixel Imaging," IEEE Access, vol. 7, no.2, pp. 119557-119565, 2019.

[9] S. Kaushik, and S. Puri, "Online transaction processing using enhanced sensitive data transfer security model," in Proc. 2012 Students Conference on Engineering and Systems, 2012, pp. 1-4.

[10] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," IEEE Access, vol. 7, pp. 134422-134433, 2019.

[11] F. Casino and C. Patsakis, "An Efficient Blockchain-Based PrivacyPreserving Collaborative Filtering Architecture," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1501-1513, Nov. 2020.

[12] D. Chkliaev, J. Hooman and P. van der Stok, "Mechanical verification of transaction processing systems," in Proc. ICFEM

2000. Third IEEE International Conference on Formal Engineering Methods, 2000, pp. 89-97.

[13] S. Zhang, and J H. Lee. “Mitigations on Sybil-based Double-spend Attacks in Bitcoin,” IEEE Consumer Electronics Magazine, vol.7, no. 2, pp. 1-1, 2020.

[14] X. Wang, Q. Feng and J. Chai, “The Research of Consortium Block chain Dynamic Consensus Based on Data Transaction Evaluation,” in Proc. 2018 11th International Symposium on Computational Intelligence and Design, 2018, pp. 214-217.

[15] S. Zhang, and J. H. Lee, “A group signature and authentication scheme for blockchain-based mobile-edge computing,” IEEE Internet of Things Journal, vol. 7, no. 5, 4557-4565, 2019.