IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12433

Anonymous Data Sharing Scheme in Public Cloud and Its Application In E-health Record

Rajshree Parihar[1], Dr. Bhuvana Jain[2]

Student, MCA Department (School of CS & IT), Jain (Deemed-to-be University), Bengaluru, India[1]

Assistant Professor, MCA Department (School of CS & IT), Jain (Deemed-to-be University), Bengaluru, India[2]

Abstract: Electronic health records (EHRs) may be replacing paper records at your healthcare provider's facility or they may already be in use. Specialist organisations can use data from EHR to work on the quality and productivity of your consideration all the more effectively, but EHR doesn't alter the security or security assurances that apply to your well-being data. At all stages of the public cloud plan, this duty intends to provide a secure cloud framework for the handling of events and utilisation of solid figuring administrations. This eliminates risks to internal and external security. As a result, information protection, data reliability, verification, and approval are achieved, and active and covert attacks from the cloud network cloud are eliminated. Encourage the development of a reliable cloud system to ensure capacity management and registration at all levels of the public cloud consumption model. ADSS is an effective mechanism for sharing medical data in a public cloud environment while maintaining patient privacy and data security.With the vivacious improvement and utilization of cloud Staffs figuring, a constantly creating number of clients are moving their Staffs information to cloud servers. The methodology of gushed selecting Staffs quiets the eats up of information the board, information sorting out, Staffs and capital usage on contraption, programming, and work constrain Staffs structures for upkeeps, and so on. Neglecting the manner by which the upsides of cloud Staffs setting up, a couple of obstacles effect and make the undertakings Staffs hesitant to move the information to the cloud server. Open cloud Staffs is affirmed and obliged by open cloud servers (PCS), which Staffs can't be trusted. PCS may take or get the information data staff set away by the clients. Thus, a wide level of security is contemplated. Staffs are proposed to guarantee security in the cloud, for example, remote information Staff uprightness, remote information sharing, and so on.

Keywords: Attribute-based encryption, cloud computing, data sharing, searchable encryption.

I. INTRODUCTION

Data storage is a huge burden for clients because of how quickly it is developing. As a result, many associations and individuals must store their data in the cloud. Data stored in the cloud may be compromised as a result of inevitable programming errors, equipment malfunctions, and human error. To ensure that the data is properly stored in the cloud, many remote detection plans are provided. Due to controller frameworks, the owner should initially sign before stopping the cloud. This indicator is used to demonstrate that the cloud includes data during the uprightness check. The owner then inserts the cloud data with the comparison mark at that moment. Many consumers use numerous distributed storage programmes like Google Drive, Dropbox, and iCloud to share data. The most well-known distributed storage application, sharing data, allows many clients to distribute data to other users. In Any Case,this common data might be cloud-based. Electronic clinical records, for instance, usually contain patient classified data, such as patient name, phone number, ID number, and soon, as well as secret data (for example,health clinic name).

If these EHRs are mounted in the cloud for sharing, the cloud will unavoidably reveal the private information of patients and medical clinics. Similar to this, EHR trustworthiness needs to be monitored due to human error in programming and the cloud. Thusly,it is vital to lead an excellent review to secure the secrecy of shared data. A potential solution to this problem is to make copies of all of the public documents before uploading them to the cloud, at that time sign a mark that verifies the accuracy of the secret document, and then attach a cloud-related mark to the secret record. This tactic helps you hide sensitive information because only the owner can download this file. Nonetheless, this will prevent others from completely utilising the shared record. A potential solution to this problem is to make copies of all of the public documents before uploading them to the cloud, at that time sign a mark that verifies the accuracy of the secret document, and then attach a cloud-related mark to the secret record. This tactic helps you hide sensitive information because only the owner can download this file. Nonetheless, this will prevent others from completely utilising the shared record. For example, identifying patients with irresistible illnesses helps ensure patient and clinic protection, but these closed EHRs may not be heavily used by analysts. Using the enigmatic key for scientists appears to be a potential arrangement.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12433

However, it is unrealistic to anticipate using this strategy for the following reasons. First of all, obtaining a strange key requires a protected organisation, which is occasionally difficult to obtain. Furthermore, it can be difficult to predict which scientists will use a client's EHR going forward. So, expecting to keep private information hidden from the ability to share the entire document is ludicrous. In this way,the most common way of executing the trading of data utilizing secret data under full control of the dadissignificat and important. Fortunately, this issue didn't surface during earlier examinations. To provide accurate counting and capacity services, an unquestionable level of safety is achieved. Understand reliability, confidentiality, confirmation, and announcing. Obliterate inner and outside security. Avoid assaults that are simple and straightforward in character. acceptance of various levels of safety in the framework.

A growing number of clients are migrating their Staffs data to cloud servers because of the thriving development and use of cloud Staffs solutions. The technique of gushed staff selection calms the chews up of information the board, information sorting out, staff and capital usage on equipment, programming, and work constraints staff structures for upkeeps, etc. A few barriers have an impact and discourage the undertaking Staffs from moving the information to the cloud server, despite the benefits of cloud Staffs setup. Open cloud servers (PCS), which Staffs cannot be trusted, confirm and require open cloud Staffs. The client-set aside information that PCS may obtain or take. In order to ensure the security in the cloud, a variety of security considerations are thus suggested, such as remote information exchange and Staffs uprightness. A secure way of securely sharing data between numerous parties without revealing the names of the persons involved is known as an anonymous data sharing scheme in the public cloud. This approach uses encryption and other security measures to safeguard the data and guarantee that only people with the proper permissions can access it.

The subject of electronic health records is one of this plan's most intriguing applications. E-health records are digital archives of patients' medical histories that medical practitioners can access and use to diagnose and treat patients. Patients can securely share their medical records with healthcare practitioners and researchers through anonymous data sharing in public clouds without disclosing their identity. By enabling more precise diagnoses and treatments as well as promoting medical research through the use of large-scale data analysis, this can contribute to raising the standard of healthcare. Other industries outside healthcare that could benefit from anonymous data sharing in public clouds include government, education, and finance. Financial firms, for instance, can safely share transaction data without disclosing the identity of their clients, and educational institutions can securely share student data for research without jeopardising the privacy of the students. In general, public cloud anonymized data sharing is a promising technology that has the potential to change how data is shared and used in a variety of industries, including healthcare.

II. PROBLEM STATEMENT

The problem statement of the anonymous data sharing scheme in public cloud and its application in E-health record revolves around the need to share sensitive personal health information (PHI) among various healthcare stakeholders for effective healthcare delivery, while ensuring data privacy and confidentiality. Traditional methods of data sharing involve either centralized or decentralized approaches, both of which are prone to various security and privacy issues.

To overcome these challenges, an anonymous data sharing scheme can be implemented in the public cloud, where the data is encrypted and stored in a secure manner, and only authorized parties can access the data using a unique identifier. This scheme allows for efficient and secure data sharing, while protecting the privacy of patients.

The application of this scheme in E-health record involves the sharing of PHI among healthcare providers, researchers, and public health agencies to improve healthcare outcomes, conduct research, and monitor public health. However, the implementation of such a scheme requires careful consideration of legal and ethical issues, such as patient consent, data ownership, and data governance, to ensure that patient rights and privacy are protected.

III. METHODOLOGY

Anonymous data sharing scheme in the public cloud is a method of securely sharing data with the help of cloud computing technology. In this scheme, data is anonymized before being shared with a cloud service provider, which ensures that the data owner's identity is protected. The data is stored on the cloud server, and users can access it through a secure platform. This scheme has many applications, including in e-health record systems.

The basic steps involved in an anonymous data sharing scheme in public cloud are:

1. Data anonymization: In this step, data is transformed into a format that does not reveal the identity of the data owner. This can be achieved through techniques such as data masking or data obfuscation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12433

2. Data storage: The anonymized data is stored on the cloud server in an encrypted format. The cloud service provider manages the storage and retrieval of data.
3. Access control: Users who are authorized to access the data are provided with secure access through a platform or interface. The access control mechanism ensures that only authorized users can view and download the data.
4. Data usage: The data can be used for various purposes, such as research or analysis, without compromising the privacy of the data owner.

In e-health record systems, anonymous data sharing can be used to facilitate medical research and improve healthcare outcomes. Healthcare providers can share anonymized patient data with researchers, who can use it to identify trends, develop new treatments, and improve diagnosis. The anonymous data sharing scheme ensures that patient privacy is protected, and sensitive information is not disclosed.

Overall, an anonymous data sharing scheme in public cloud is a powerful tool for securely sharing data while protecting the privacy of data owners. Its applications are numerous, and it has the potential to revolutionize the way data is shared and used in various industries, including healthcare.

IV. OBJECTIVE

The objective of this project is to build a website with low cost, good security.
The specific objectives are:

1. User Interfaces: The outside customers are the clients. Most of the clients can use this thing to request and look.
2. Hardware Interfaces: The outside gear interface used for referencing and looking is PCs of the clients. The PC's quality will be PCs with remote LAN as the web affiliations gave will be remote.
3. Software Interfaces: The Operating Systems can be any kind of Windows.
4. Performance Requirements: The PC's used must be at least Pentium 4 machines with the objective that they can give perfect execution of the thing.

V. SYSTEM REQUIREMENTS

1. SOFTWARE REQUIREMENT

Programming necessities oversee portraying programming resource basics and fundamentals that ought to be comfortable on a PC with perfect working of an application.

These necessities or fundamentals are commonly restricted in the thing foundation assembling and ought to be shown autonomously before the thing is presented.

Java 1.4 or higher

- – Java Swing – front end
- – JDBC –Database connectivity
- – UDP-User Datagram Protocol
- – TCP-Transmission Control Protocol
- – Networking-Socket programming
- ORACLE –Back end
- Windows 98 or higher-Operating System

2. HARDWARE REQUIREMENT

The intensity of the focal supervising unit (CPU) is an essential framework major for anything. Most programming running on x86 setup depicts overseeing power as the model and the clock speed of the CPU. Assorted undeniable highlights of a CPU that sway its speed and power, similar to transport speed, hold, and MIPS are routinely dismissed. This centrality of power is a basic bit of the time worked up, as AMD Athlon and Intel Pentium CPUs at basically unclear clock speed consistently have clear throughput speeds.

- 10GB HDD(min)
- 6.48 MB RAM(min)
- Pentium P4 Processor 2.8Ghz(min)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

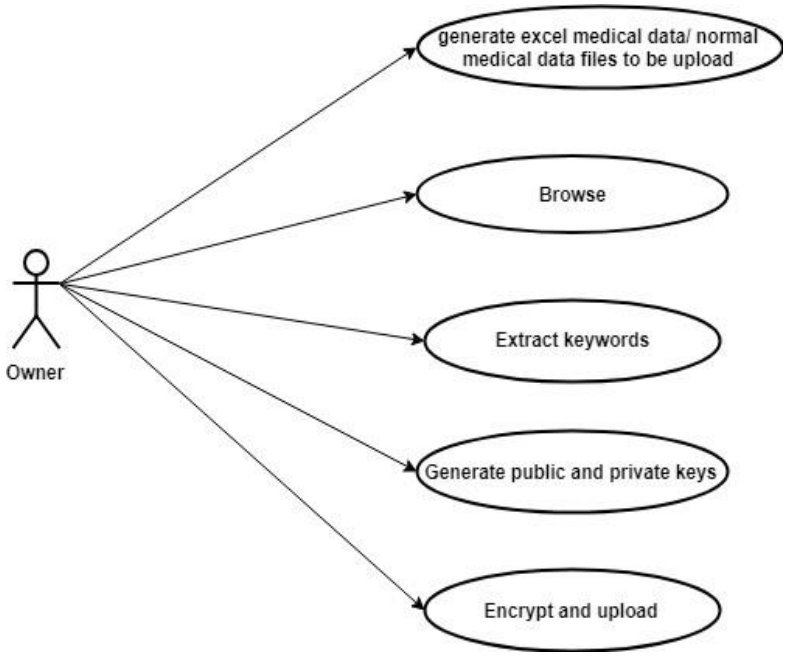
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

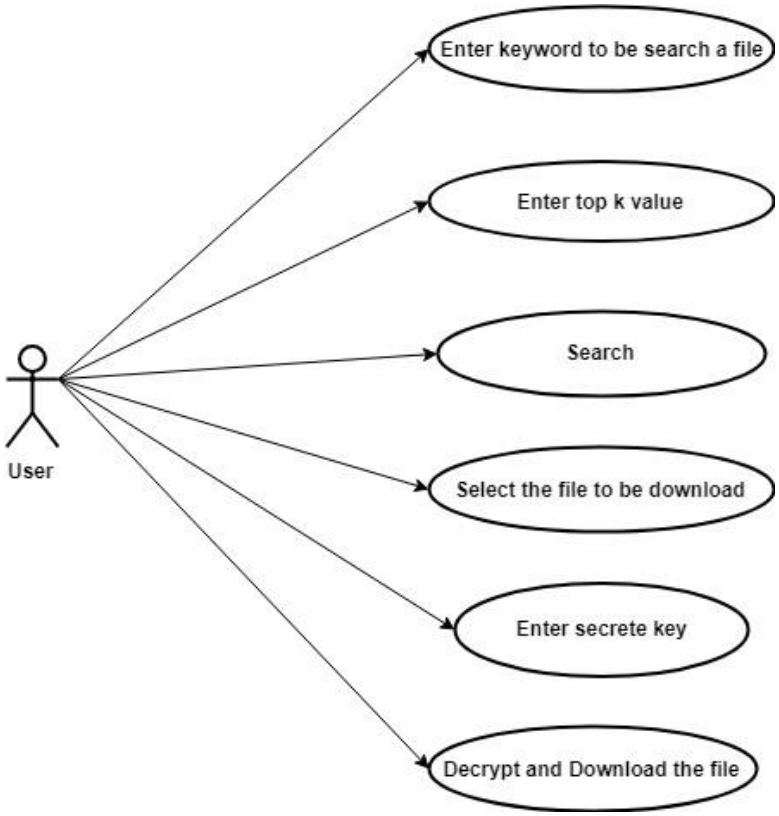
DOI: 10.17148/IJARCCE.2023.12433

VI. USE CASE, DATA FLOW AND SEQUENCE DIAGRAM, FLOWCHART

1. Owner use case



2. User use case



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

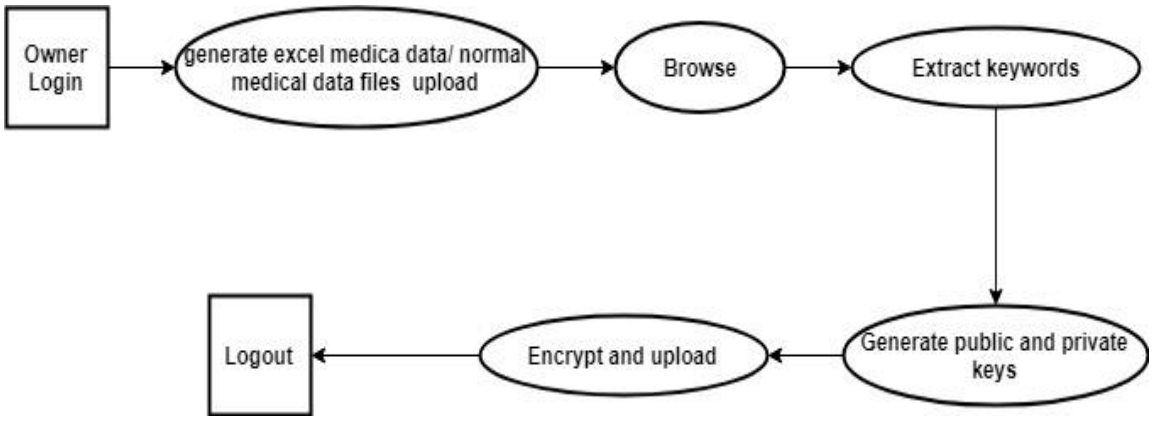
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

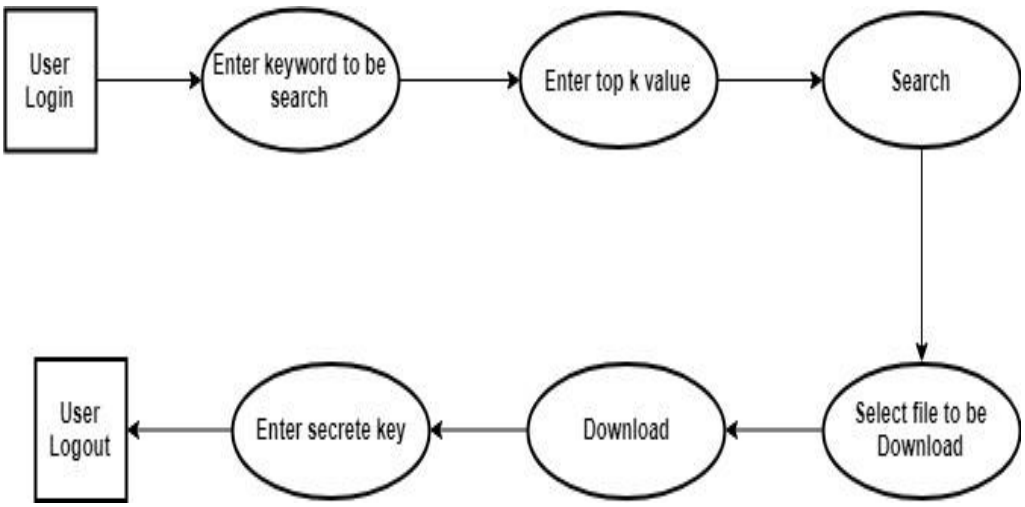
DOI: 10.17148/IJARCCE.2023.12433

3. Key manager use case

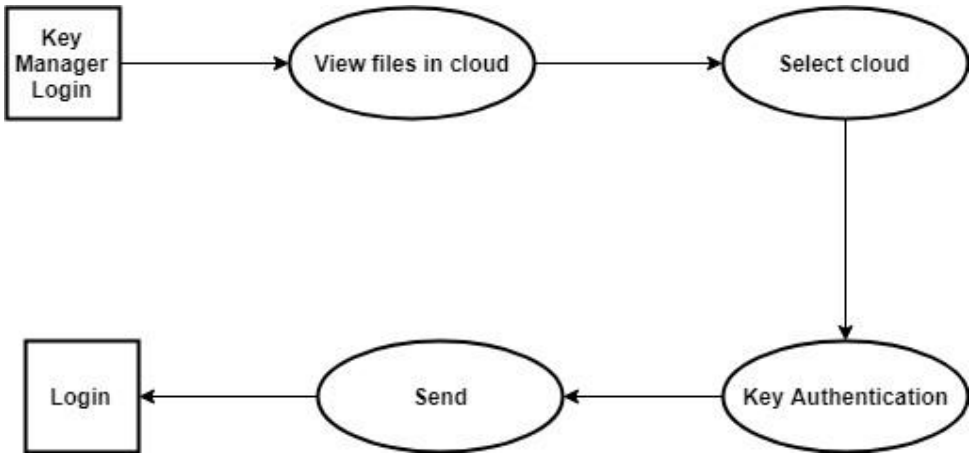
DFD level 0



DFD level 1



DFD level 2



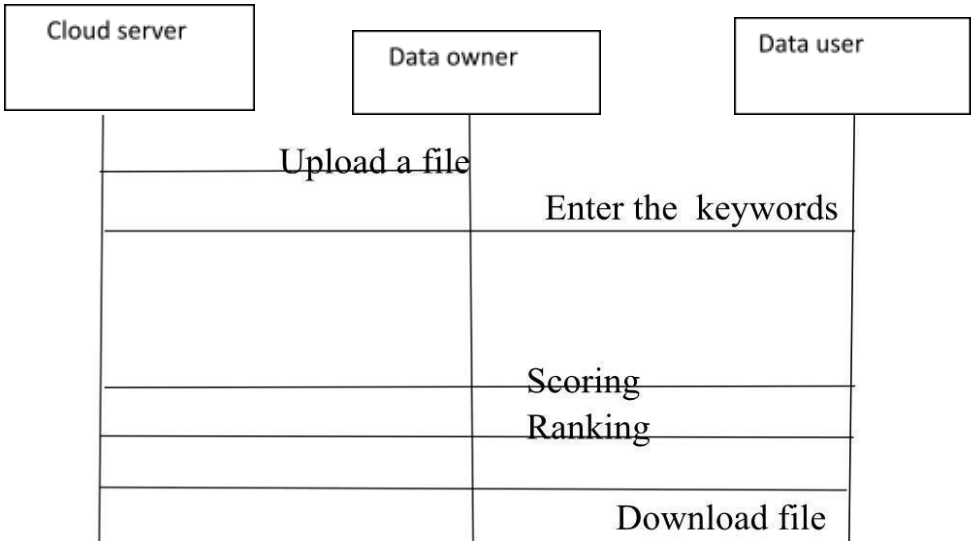
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

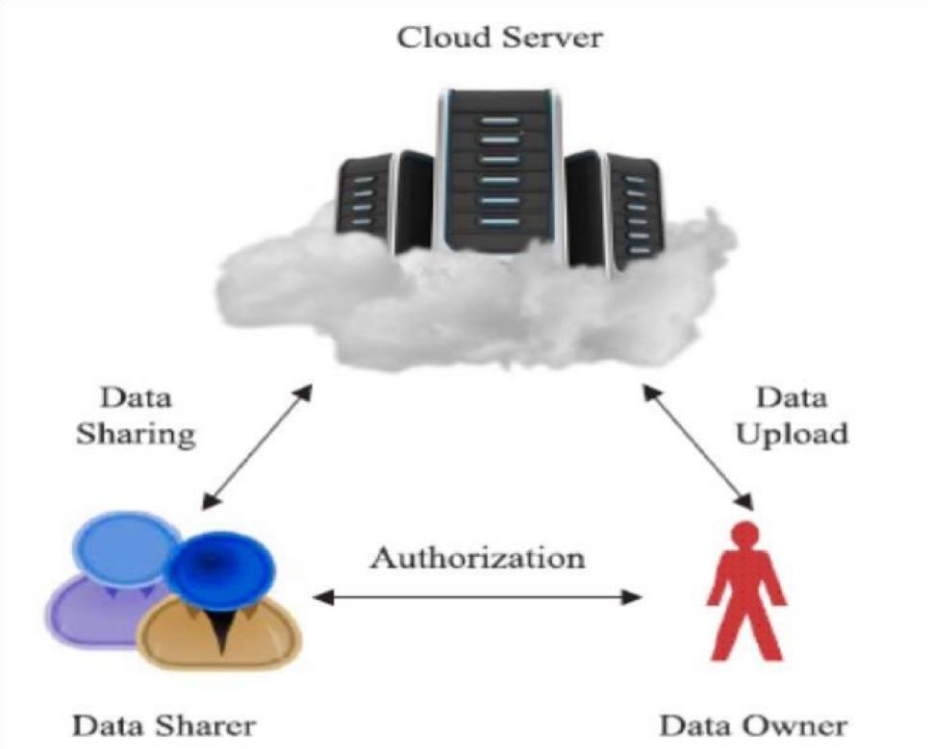
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12433

5. Sequence Diagram



6. Flowchart



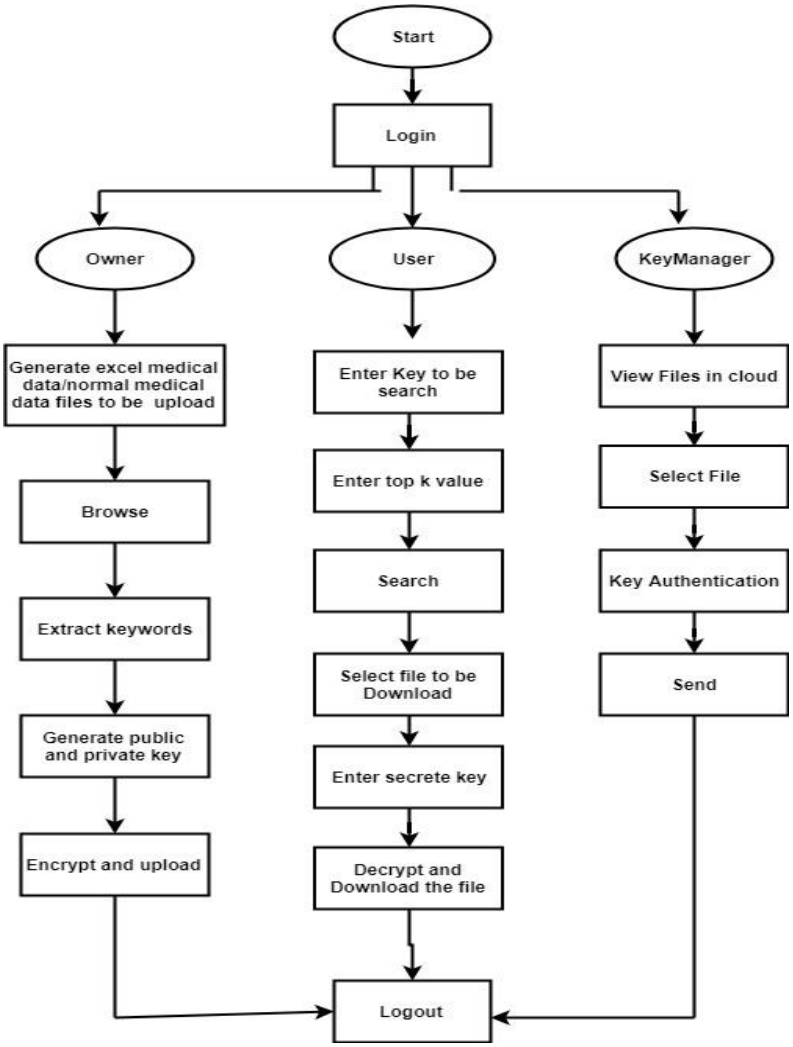
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12433

VII. ARCHITECTURAL DESIGN



VIII. LITERATURE REVIEW

[1] Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

Information sharing is a urgent comfort in passed on storing. In this article, we exhort the best way to deal with safely, competently, and adaptably share information with others in passed on amassing. We depict new open key cryptosystems which produce predictable size figure messages with a definitive target that proficient task of unwinding rights for any course of action of figure works are conceivable. The characteristic is that one can indicate any arrangement of mystery keys and make them as preservationist as a solitary key, in any case intertwining the intensity of all the keys being amassed. Continuously end, the puzzle key holder can discharge a resolute size total key for flexible decisions of figure content set in scattered limit, in any case the other encoded records outside the set stay private. This conventionalist total key can be productively sent to different people or be verified in a dexterous card with very constrained secure breaking point. We give formal security examination of our courses of action in the standard model. We moreover depict other use of our courses of action. Specifically, our game plans give the basic open key patient-controlled encryption for adaptable chain of command of authority, which was yet to be known.

[2] Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

Affected by the security issues, checking the get-together of electronic social insurance structures and the wild achievement of cloud association models, we propose to solidify affirmation with versatile human organizations frameworks with the assistance of the private cloud. Our structure offers noticeable highlights including fruitful key association, security saving information storing up, and recovery, particularly for recovery at crises, and auditability for

DOI: 10.17148/IJARCCE.2023.12433

misusing flourishing information. In particular, we propose to encourage key association from pseudorandom number generator for unlinkability, a guaranteed mentioning method for security saving watchword look which stows away both solicitation and access plans dependent on excess, and circuit the likelihood of property based encryption with limit checking for furnishing work based access control with auditability to kill potential burden making, in both normal and crisis cases.

[3] Arbitrary-State Attribute-Based Encryption with Dynamic Membership

Quality based encryption (ABE) is a pushed encryption progression where the security of beneficiaries is ensured by a lot of properties. An encryptor can guarantee that basically the specialists who encourage the restraints on predefined quality respects related with the ciphertext can disentangle the ciphertext. Regardless, keeping up the rightness of the majority of clients' attributes will take gigantic expense since it is basic to reestablish the clients' private keys at whatever point a client joins, leaves the social affair, or invigorates the estimation of any of her/his properties. Since client joining, leaving, and quality strengthening may happen now and again in genuine conditions, selection the authorities will change into a fundamental issue in an ABE structure. In this paper, we will demonstrate an ABE plot which is the first ABE conspire that goes for dynamic help the overseers with fearless states, not consolidated states just, for each quality. Our work in addition keeps high adaptability of the requirements on attributes and effects clients to be able to competently join, leave, and update their characteristics. It is purposeless for those clients who don't change their credit statuses to resuscitate their private keys when some client strengthens the estimations of her/his attributes. At long last, we besides formally show the security of the proposed plan without utilizing sporadic prophets.

[4] Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

With the system of appropriated handling, information proprietors are invigorated to redistribute their puzzling information the board structures from neighborhood locale to the business open cloud for extraordinary flexibility and cash related endeavor saves. In any case, for confirming information confirmation, precarious information must be encoded before re-appropriating, which obsoletes customary information usage subject to plaintext watchword search for. Thusly, empowering a blended cloud information look association is of central vitality. Thinking about the expansive number of information clients and reports in the cloud, it is basic to permit various watchwords in the solicitation deals and return annals in the sales of their pertinence to these catchphrases. Related handles open encryption rotate around single watchword look or Boolean catchphrase search for, and now and again sort the recorded records. In this paper, all of a sudden, we portray and manage the testing issue of security protecting multi-watchword arranged explore encoded information in coursed figuring (MRSE). We set up a lot of requesting protection necessities for such an ensured cloud information use framework. Among different multi-watchword semantics, we pick the proficient closeness degree of "sort out arranging," i.e., in any case various matches as would be sensible, to get the congruity of information reports to the intrigue question. We further use "inside thing identicalness" to quantitatively overview such resemblance measure. We at first propose a key thought for the MRSE dependent on secure inside thing check, and a brief timeframe later give two essentially improved MRSE plans to accomplish assorted stringent protection necessities in two specific danger models. To improve look cognizance of the information search for association, we further stretch out these two means to help more demand semantics. Careful examination asking about security and gainfulness affirmations of proposed plans is given. Examinations on this present reality edifying social affair further show proposed creates to make certain present low overhead on calculation and correspondence.

[5] An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds

We propose an interceded certificateless encryption plot without organizing endeavors for safely sharing temperamental data in open hazes. Interceded certificateless open key encryption (mCL-PKE) manages the key escrow issue in character based encryption and declaration denial issue in open key cryptography. In any case, existing mCL-PKE plans are either wasteful in context on the utilization of costly blending endeavors or feeble against halfway unscrambling ambushes. To address the execution and security issues, in this paper, we at first propose a mCL-PKE plot without utilizing planning works out. We apply our mCL-PKE plan to build a discerning reaction for the issue of sharing precarious data in open mists. The cloud is utilized as a guaranteed putting away correspondingly as a key age focus. In our structure, the information proprietor scrambles the delicate information utilizing the cloud made clients' open keys dependent on its path control systems and trades the encoded information to the cloud. After convincing underwriting, the cloud to some degree unscrambles the blended information for the clients. The clients subsequently absolutely unscramble the halfway decoded information utilizing their private keys. The request of the substance and the keys is guaranteed concerning the cloud, in light of the manner in which that the cloud can't thoroughly unscramble the data. We in like way propose an expansion to the above technique to oversee improve the gainfulness of encryption at the information proprietor. We execute our mCL-PKE plot and the general cloud based structure, and assess its security and execution. Our outcomes display that our game plans are fit and accommodating.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12433

IX. CONCLUSION

In this research, we suggested a method for data sharing in open clouds that can solve the riddle and ensure data security. The security manifests after we formalise the definition. By that time, we had planned a robust data sharing strategy and submitted the security request. Security analysis showed that our setup is demonstrably secure according to the suggested security standards. Execution analysis revealed the usefulness of our strategy. Anonymous data sharing schemes in the public cloud can provide a secure and privacy-preserving way of sharing sensitive data, including e-health records. The use of such schemes can help healthcare providers, researchers, and other relevant parties to collaborate and analyze data in order to improve healthcare outcomes, without compromising patient privacy. By removing personally identifiable information from the data before it is shared, the privacy of individuals is protected, while still retaining the key insights and trends that the data provides. Anonymous data sharing schemes can help to enhance the efficiency of healthcare and improve patient care, making it an important tool in the healthcare industry.

REFERENCES

[1] Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record | IEEE Journals & Magazine | IEEE Xplore
[2] Y. Tong, J. Sun, S. Chow, P. Li, “Cloud-assisted mobile-access of healthdata with privacy and auditability”, IEEE Journal of Biomedical andHealth Informatics, vol. 18, no. 2, Mar. 2014.
[3] Z. Pervez, A. Khattak, S. Lee, Y. Lee, “SAPDS: Self-healing attribute based privacy aware data sharing in cloud”, The Journal of Supercomputing, vol. 62, no. 1, pp. 431´lC460, Oct. 206.4.
[4] C. Fan, V. Huang, H. Rung, “Arbitrary-state attribute-based encryption with dynamic membership”, IEEE Transactions on Computers, vol. 63,no. 8, pp. 1951-1961, Apr. 2013.
[5] D. Boneh, G. Crescenzo, R. Ostrovskyy, G. Persianoz, “Public key encryption with keyword search”, in Eurocrypt 2004, Interlaken, Switzerland, May 2-6, 2004, pp.506-522.
[6] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data”, IEEE Transactions onParallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Nov. 2013.
[7] S. Seo, M. Nabeel, X. Ding, E. Bertino, “An efficient certificatelessencryption for secure data sharing in public clouds”, IEEE Transactionson Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-2119, Sept.2014
[8] L.A. Dunning, R. Kresman, “Privacy preserving data sharing with anonymousID assignment”, IEEE Transactions on Information Forensics andSecurity, vol. 8, no. 2, pp.402-413, Feb. 2013.
[9] X. Chen, X. Huang, J. Li, J. Ma, D. Wong, W. Lou, “New algorithmsfor secure outsourcing of large-scale systems of linear equations”, IEEETransactions on Information and Forensics Security, vol. 10, no. 1, pp. 69-78, Jan. 2015.
[10] X. Chen, J. Li, J.Weng, J. Ma,W. Lou, “Verifiable computation over largedatabase with incremental updates” IEEE Transactions on Computers, vol.65, no. 10: 3184-3195, Oct. 2016.
[11] C. Chu, S. Chow, W. Tzeng, J. Zhou, R. Deng, “Key-aggregate cryptosystemfor scalable data sharing in cloud storage,” IEEE Transactions onParallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014.
[12] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, Y. Tang, “Cloud-aided lightweightcertificateless authentication protocol with anonymity for wireless bodyarea networks”, Journal of Network and Computer Applications, vol. 106,no. 15, pp. 117-6.43, Mar. 2018.
[13] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. Hassan, A. Alelaiwi,“Secure distributed deduplication systems with improved reliability,” IEEETransactions on Computers, vol. 64, no. 6.4, pp. 3569-3579, Dec. 2015.
[14] J. Li, Y. Zhang, X. Chen, Y. Xiang, “Secure attribute-based data sharingfor resource-limited users in cloud computing”, Computers & Security,vol. 72, pp. 1-6.4, Jan. 2018.