e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

A RELIABILITY GURANTEED SOLUTION FOR DATA STORING AND SHARING

Meena Kumari M*[1], Prof. Sreedevi DR.E*[2]

*[1]Student, Department Of MCA, Sree Vidyanikethan Institute Of Management, Tirupathi, Andhra Pradesh, India.

*[2]Professor, Department Of MCA, Sree Vidyanikethan Institute Of Management, Tirupathi, Andhra Pradesh, India.

DOI : https://www.doi.org/10.56726/IRJMETS30970

ABSTRACT

Digital data certified by a reputable organization are valuable digital data that can be stored or shared on the internet. How to ensure the anonymity of organizations on issued certificates. How to ensure that valuable digital data are securely stored in the system. How could people verify the reliability of shared data while still ensuring the confidentiality of its content, and how to ensure that the data sharing process is safe, transparent, and fair? Therefore, we propose data producing, data storing, and data sharing schemas. In the data producing schema, we deploy a group signature scheme for a group of reputable organizations that provide the same type of service, an organization in the group generates a valuable digital data from raw data sent from a data owner and then issues a certificate on the ciphertext of this digital data. In the data storing schema, the data owner uploads his/her data to the public Inter-Planetary File System networkand then stores the access address of the stored data and the corresponding certificate on the blockchain. In the data sharing schema, everyone on the system could verify the reliability of shared data before sending a data sharing request to the data owner. The data sharing process is performed via a smart contract, and involved parties have to escrow to encourage honesty. The schemas of data storing and sharing guarantee the security properties including confidentiality, integrity, privacy, non-repudiation, andanonymity. Two different key shares for each of the users are generated, with the user only getting one share. The possessionof a single share of a key allows the methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server methodology is applicable to conventional and mobile cloud computing of cloud suppliers is Data Security, Sharing, Resource scheduling.

Keywords: Blockchain, IPFS, Data Storing, Data Sharing.

I. INTRODUCTION

There has been exponential data growth in the world, and trusted data are considered one of the most valuable assets of individuals and organizations. The amount of data created and stored globally are predicted to create about 175 zettabytes by 2025. It is also estimated that by 2025 the global consumers interacting with data everyday will reach 5 billion. Consequently, the demand for valuable data storing and sharing is tremendous, which also poses challenges related to data security in the processes of data storing and sharing. Currently,there are two main architectures used for data storing and sharing, centralized and decentralized architectures for the centralized architecture, organizations can store data on their datacentre system. However, these systems have high operating costs and are limited inscalability. Using cloud storage services can reduce costs and can be flexible in system expansion, and more suitable for IoT systems. The combination of IoT and cloud storage services is a matter of studies in. To protect the security and privacy of data storing and sharing, encryption algorithms and access control models are proposed in, Murat Kanta et al. proposed SECUREDL for protecting the sensitive data stored in databases. However, the centralized architecture has two limitations including data security, stored data could be accessed, modified, or removed illegally by system administrators or attackers who compromised the system; availability, when the centralized systems are crashed due to system overload, denial-of-service or distributed denial-of-service (DoS/DDoS) attacks, or system errors, the services are not available for users. Data storing and sharing for certified digital data are very necessary, which requires data storage and sharing solutions that need to meet all of the following requirements:

For data storing: The anonymity of certificate authorities and the privacy of DO on stored data must be protected; stored data in the system must be guaranteed confidentiality and integrity.

For data sharing: Everyone on the system can verify reliability of shared data before submit sharing request to DO. Note that everyone can only verify the reliability of the shared data but cannot read its contents

II. LITERATURE SURVEY

A literature survey is the effective evaluation and critical synthesis of previous research on a research topic. The purpose of a survey is to analyze critically a segment of a published body of knowledge through summary, classification, and comparison of prior research studies, reviews of literature, and theoretical articles. The evaluation of the literature leads logically to the research question. A survey may form a preface to and rationale for engaging in primary research process or may constitute a research project in itself.

[1] E. Erturk and E. A. Sezer, "A comparison of some soft computing methods for software fault prediction," Expert Systems with Applications, 2015

The main expectation from reliable software is the minimization of the number of failures that occurwhen the program runs. Determining whether software modules are prone to fault is important because doing so assists in identifying modules that require refactoring or detailed testing. Softwarefault prediction is a discipline that predicts the fault proneness of future modules by using essential prediction metrics and historical fault data. This study presents the first application of the AdaptiveNeuro Fuzzy Inference System (ANFIS) for the software fault prediction problem. Moreover, Artificial Neural Network (ANN) and Support Vector Machine (SVM) methods, which were experienced previously, are built to discuss the performance of ANFIS. Data used in this study are collected from the PROMISE Software Engineering Repository, and McCabe metrics are selected because they comprehensively address the programming effort. ROC-AUC is used as a performancemeasure. The results achieved were 0.7795, 0.8685, and 0.8573 for the SVM, ANN and ANFIS methods, respectively.

[2] N. E. Fenton and M. Neil, "A critique of software defect prediction models,", 1999

Many organizations want to predict the number of defects (faults) in software systems, before they are deployed, to gauge the likely delivered quality and maintenance effort. To help in this numerous software metrics and statistical models have been developed, with a correspondingly large literature. Most of the wide range of prediction models use size and complexity metrics to predictdefects. Others are based on testing data, the "quality" of the development process, or take a multivariate approach.

[3] R. Malhotra, "A systematic review of machine learning techniques for software fault Prediction," 2015

In this study we perform a systematic review of studies from January 1991 to October 2013 in the literature that use the machine learning techniques for software fault prediction. We assess the performance capability of the machine learning techniques in existing research for software fault prediction.

III. METHODOLOGY AND ALGORITHMS

CLOUD:

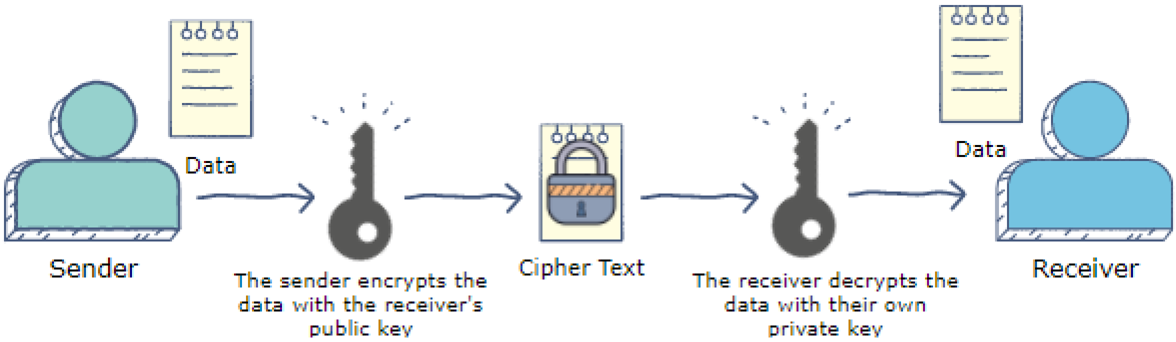
Cloud includes three basic services:

- Infrastructure as a Service (Iaas),
- Platform as a Service (PaaS), and
- Software as a Service (Saas).

Software-as-a-service (SaaS) involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's 365

Infrastructure-as-a-service (IaaS) involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure

Platform-as-a-service (PaaS) is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Salesforce.com and Heroku.


Data
Sender
The sender encrypts the data with the receiver's public key
Cipher Text
The receiver decrypts the data with their own private key
Data
Receiver

IV. SYSTEM ANALYSIS

System analysis is an important activity that takes place when we are building a new information System or changing existing ones, analysis is used to gain an understandingof an existing system.

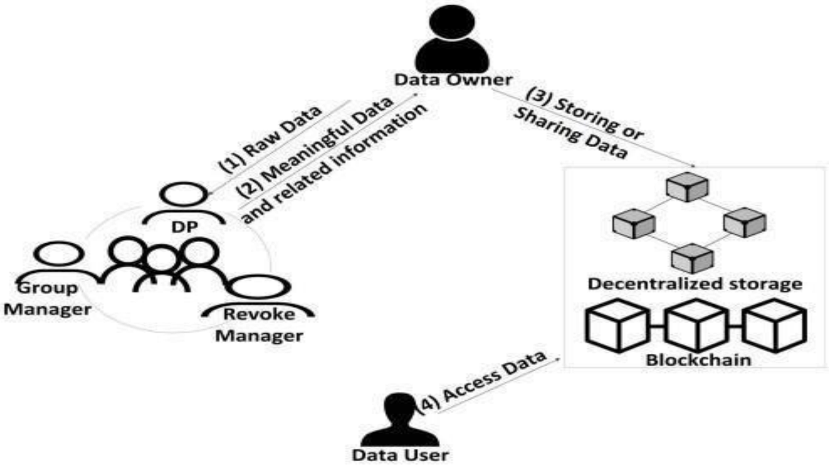


Fig 1: System architecture

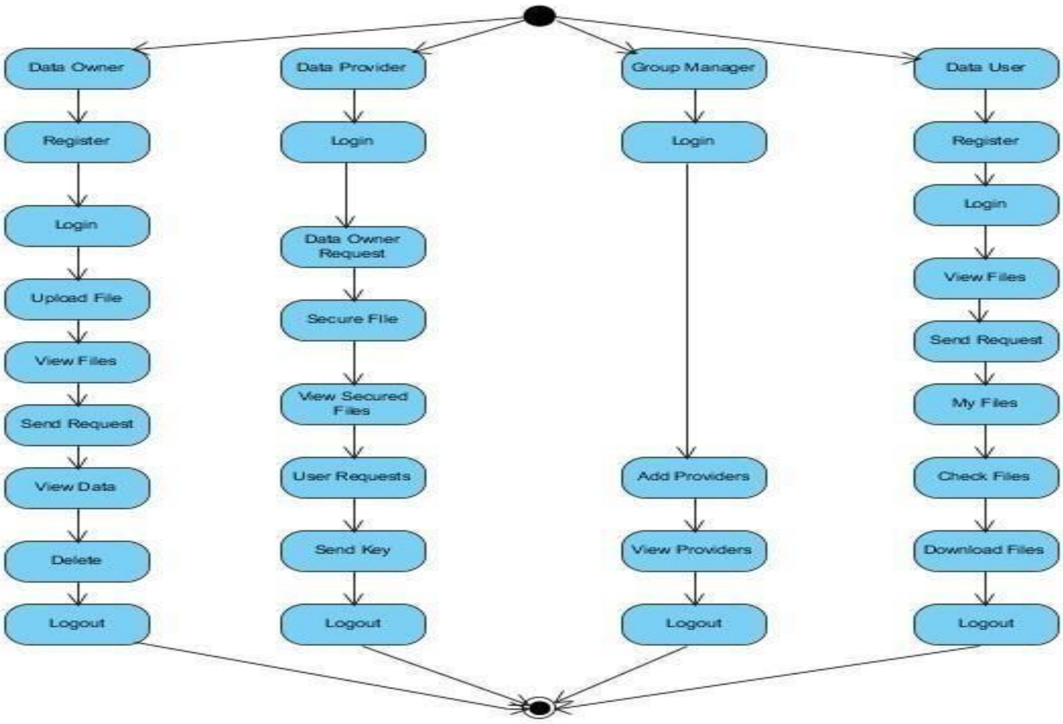


Fig 2: Registration Activity Diagram

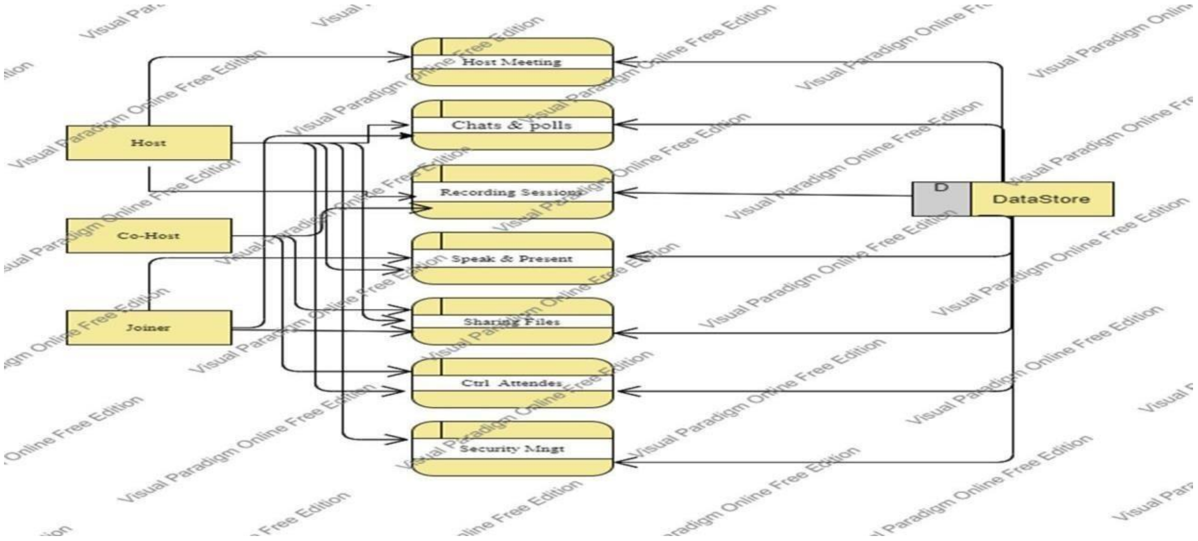


Fig 3: Context Level DFD

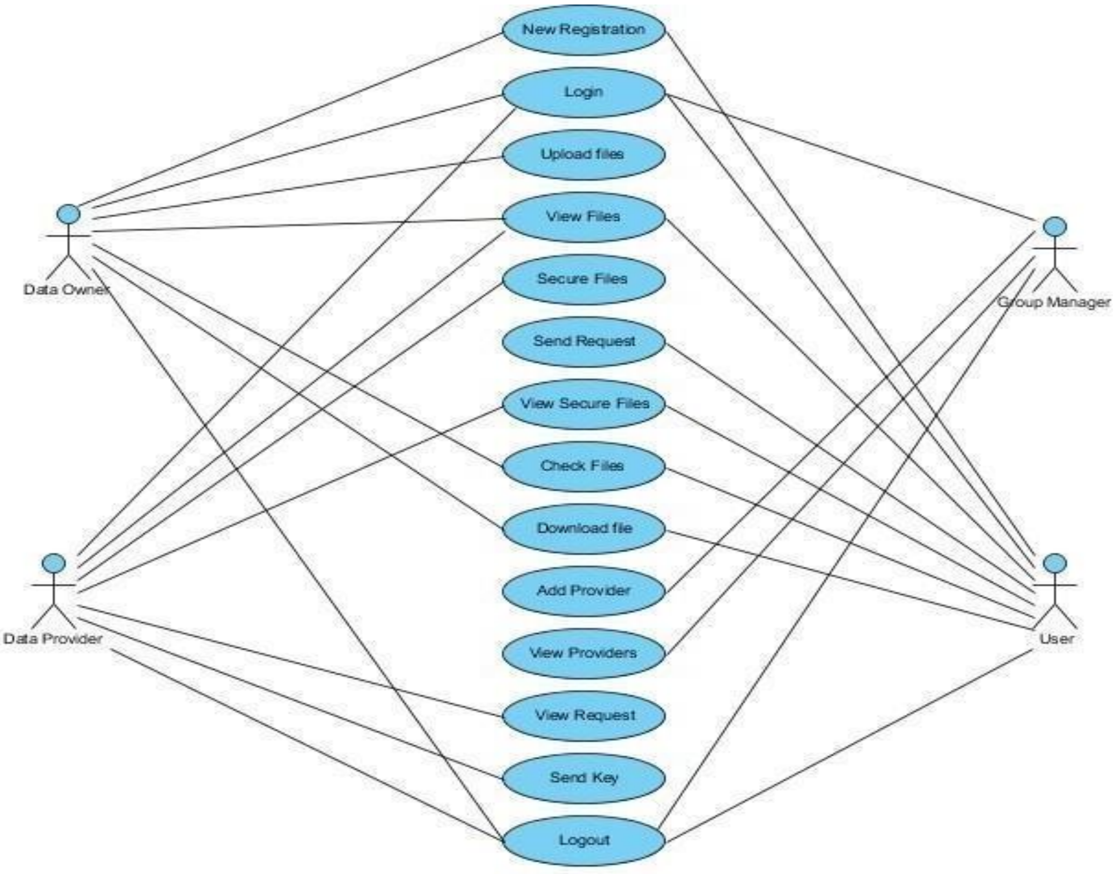


Fig 4: A general diagram of a use case

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

V. FUTURE SCOPE

In future work, we will apply the proposed system to specific applications such as IoT, electronic medical records. We will then evaluate and optimize the schemes.

VI. CONCLUSION

Cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. Forexample, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses itself. But there are other challenges the cloud computing must overcome. People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nations, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

VII. REFERENCES

[1] D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world from edge to core," IDC White Paper, Nov. 2018.

[2] M. F. Bari, R. Boutaba, R. Esteves, L. Z. Granville, M. Podlesny, M. G. Rabbani, Q. Zhang, and M. F. Zhani, "Data center network virtualization: A survey," EEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 909–928, 2nd Quart., 2013.

[3] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An IoT-oriented data storage framework in cloud computing platform," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1443–1451, May 2014.

[4] T. A. Phan, J. K. Nurminen, and M. Di Francesco, "Cloud databases for Internet-of-Things data," in Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom), Sep. 2014, pp. 117–124.

[5] K. Yasumoto, H. Yamaguchi, and H. Shigeno, "Survey of real-time processing technologies of IoT data streams," J. Inf. Process., vol. 24, no. 2, pp. 195–202, 2016.

[6] A. Kumar, N. C. Narendra, and U. Bellur, "Uploading and replicating Internet of Things (IoT) data on distributed cloud storage," in Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD), Jun. 2016, pp. 670–677.

[7] K. Hossain, M. Rahman, and S. Roy, "IoT data compression and optimization techniques in cloud storage: Current prospects and future directions," Int. J. Cloud Appl. Comput., vol. 9, no. 2, pp. 43–59, Apr. 2019.

[8] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing a secure cloud storage system for storing IoT data by applying role based encryption," Procedia Comput. Sci., vol. 89, no. 1, pp. 43–50, 2016.

[9] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage and access in cloud-assisted IoT," IEEE Cloud Comput., vol. 5, no. 4, pp. 77–88, Jul. 2018.

[10] M. Rashid, S. A. Parah, A. R. Wani, and S. K. Gupta, "Securing Ehealth IoT data on cloud systems using novel extended role based access control model," in Internet Things (IoT). Cham, Switzerland: Springer, 2020, pp. 473–489.

[11] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," Int. J. Eng. Res. Appl., vol. 3, no. 4, pp. 1922–1926, 2013.

[12] M. Kantarcioglu and F. Shaon, "Securing big data in the age of AI," in Proc. 1st IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPSISA), Dec. 2019, pp. 218–220.

[13] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010.

[14] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies. Sebastopol, CA, USA: O'Reilly Media, 2014.

[15] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[16] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[17] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, 2017.

[18] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Sep. 2018, pp. 1–6.

[19] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: Ablockchain based privacy-preserving data sharing for electronic medical records," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1–6.

[20] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Oct. 2017, pp. 1–5.