International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ACCESS CONTROL BY SIGNATURE-KEYS TO PROVIDE PRIVACY FOR CLOUD

[1]Gajam Shekar, [2]K Pranaya Vardhan, [3]D Shiva Prasad Goud, [4]Morgu VaishnavI

[123]Assistanct Professor, [4]UG Scholar, Department of CSE, Brilliant Institute of Engineering & Technology, Abdullapurmet(V&M) Ranga Reddy Dist-501505

ABSTRACT

Privacy of data in subjects of cloud computing or big data is one of the most principal issues. The privacy methods studied in previous research showed that privacy infringement for cloud computing or big data happened because multi risks on data by external or internal attackers. An important risk to take into consideration when speaking of the privacy of the stored transactions is represented by the transactions' information which is not in the owner's control. Such a case is represented by the cloud servers that are administered by cloud providers which cannot be wholly trusted by the users with sensitive, private data such as business plans or private information. A simple method for protecting data privacy is by applying certain privacy techniques onto transactions' data, followed by the upload of the modified data into the cloud. In this paper, we are proposing a case study that is built on levels containing three models: cloud's architecture, transaction's manager and clients. Moreover, we consider that our case study is based on the premise of zero trust among the three models, therefore all the transactions take place with third-parties and the data movements are realized going through various levels of security.

I.INTRODUCTION

Cloud computing and Big data as novel techniques need more attention and research. The privacy for these novel techniques is one of the most important issues. Shared data or processing and transferring data in third party could is more vulnerable to attacks, such as sync cookies, attacks on client profiles, limited connections of provided, etc. [1]. Cloud computing is seen as an essential, low-maintenance way to share resources. More and more, moving the systems that manage the local information into cloud servers has become the standard procedure, clients being able to benefit of premium services whilst saving big money on the local infrastructures. Users that use cloud computing are no longer faced with the disadvantages of the problematic local solutions for storing and management of data. Using policy of encrypted data based on access control is the most common privacy method. This policy cab ensures privacy of data that represent sensitive information. The privacy based on access control means to allow access to data only to authorized persons. The access mechanisms to the sensitive data have problems if they can be shared without strong privacy. Data is often in cloud or big data with shared access with third party, which makes it more vulnerable to attacks. Usually, moving data between sides can be risky on client privacy. To ensure end-to-end security, we try to implement algorithms to provide strong privacy for big data in cloud. Other related works and research in same area, as the encryption based-attribute, show the most suitable

approach to identify efficient and more scalable methods. Cloud computing implies a set of computers that are used together to provide different accounts and services. The benefits of using cloud computing in companies are cost reduction and time saving. Also, using shared services from cloud is easier than building and developing own infrastructure. The providers of cloud computing are focus on providing flexible services, cost-effective IT infrastructure and secure environments for companies and organizations [4]. The main issue with big data in cloud is that processing or usage always needs to be done by third party. It is very important for the owners of data, or clients, to trust and to have the guarantee of privacy for the information stored in cloud or analyzed as big data. The privacy methods studied in previous research showed that privacy infringement for cloud computing and big data happened because of limitation, privacy guarantee rate or risks on data by external or internal attackers. Generally, the private client data has been under attack

Cloud computing, big data and privacy include many issues that need to be examined, analyzed and processed in order to obtain the optimum combination for providing strong privacy for clients.

a)Cloud computing general information

Cloud computing implies a set of computers that are used together to provide different accounts and services. In general, cloud computing includes two sides [2] [3] - the first one is the front end used by users and clients and the second one is the environment behind the providers' location. The application interface varies for users and it depends on the cloud services provided to the clients. Despite the diversity of applications, they are often united in privacy requirements. The benefits of using cloud computing in companies are cost reduction and time saving. Also, using shared cloud services is easier than building and developing own infrastructure. The providers of cloud computing focus on providing flexible services, cost-effective IT infrastructure and secure environments for companies and organizations [4]. b)Big data general information Big data is massive structured and unstructured data. In order to process it, a huge environment is needed because processing by normal databases or using any systems is quite difficult [3]. The dimensions of big data include velocity, volume, and variety. These dimensions need to be handled through designing large and effective systems. Big data are classified into passive and active data generation. Passive data is the data generated only during the client's online activity or interaction with systems. This kind of data can be collected and used by third party without clients' awareness. Active data generation is provided directly from clients to be used by third party [5]. c) Privacy methods general information Privacy in general refers to control of information and usage permissions, which include users and amount of allowed data to be accessed. Privacy is the right to reach and use personal information, location and private data for which has been granted access to use. In case access is granted, the party accessing the data must also control any other accessing party against accidental data privacy loss or unauthorized access. The accessing party is responsible for any subsequent use, sale or manipulation of the data. Researchers work to find ways to solve

privacy issues and avoid intentional or unintentional violation. To achieve these goals, they classified privacy protection in two categories – the first is protected access to data and relevant protected mechanisms and the second is obscuring private data from not allowed usage. 1. Access control methods i. Identity management and access control Identity management: includes authentication, authorization and user control processes. In order to detect identity, the system should protect access to data and deny users that are not allowed access. Providers of cloud services are responsible to customize the available authentication and supports basic (login/manage accounts/password) authentication. In addition, some access control management provides unique Key-ID to new users to grant data usage at first login [6]. ii. Authentication and authorization Authentication and authorization: is an important method of data protection in any system. Various authentication and authorization styles have been implemented and proposed for user data protection. For examples, in [9] the study provided a way to develop models using multi-factor authentication and implementation in cloud. The study also focused on controlling the appropriate requirements, categories, services identified in cloud for authorized users. FemiCloud [10] adopted another approach using authentication and authorization. They developed the approach using public key (PKI) X.509 certificates provided for detecting users' identity for authentication. A web interface built by FemiCloud provides certificates for users' management. 2. Private data hiding methods i. K-anonymity To protect private data, we can use other methods that obscure part of data. These methods can provide high privacy when applied the right way. The k-anonymity is one of the most common of these methods. In 2002 K-anonymity was proposed by Sweeney [11], and in 2008 was further developed by Lodha and Thomas [12]. The aim of k-anonymity is to hide part of data sets by restricting the intruders and denying disclosure of private data. The purpose of k-anonymity is to block any cases of clients' identity disclosure. Also, the objective of kanonymity is to create sets of quasi-identifiers in results of the anonymized data to indicate at least k-tuples, which are purported equality tuples[24]. ii. Differential-privacy Differential-privacy is one of the privacy methods used for anonymization, which provides privacy safeguards more than other models, such as k-anonymity, T-Closeness or Ldiversity [13][24]. Differential-privacy implies publishing the results of a query with some noise added to the results of the query. In this case, the attacker can't guess the results of the query because it contains noise with 100% guarantee. Differential-privacy has several drawbacks. The first major impediment is that differential privacy fails to give assurances with dataset linkage and attribute in data. Usually, this model is preferred in cases where the result of congruence queries is few and with low sensitivity. This makes differential-privacy the best in restricted classes of queries [14]. This model was initially proposed by Cynthia Dwork in 2008 [15], [16]. I. RELATED WORKS AND BACKGROUND Cloud computing and Big data have the same details and properties, as well as the issue of privacy maintenance, especially when these data are used by third party. Many related works have reached

good results in solving the same problem as the present study. [7] [8] Subashini et al. suggested a metadata established on segregation technique and storage methodology. They proposed protecting from concerns of attacks on the data stored in the cloud using model segregation of the data. The data value in cloud gained during acquisition is separated in multi-location to support privacy of clients. Access to data in cloud presents no risk since loading and using the data is allowed

II.LITERATURE SERVEY

In the realm of cloud computing, the management and security of sensitive data have become pressing concerns due to the pervasive and cost-effective nature of cloud services. The paper by Ulrich Xzzzq, Benjamin Justus, and Dennis Loehr (2011)**, titled *"A Privacy Preserving System for Cloud Computing"*, addresses these concerns by proposing a novel cloud database storage architecture. This system is designed to enhance privacy by ensuring that both local and cloud administrators cannot access the outsourced database content. It incorporates machine-readable rights expressions to restrict database access to only those with a need-to-know basis. Importantly, once an application is launched, the permissions and roles defined cannot be altered by administrators, as a new role of rights editors is established. Additionally, the paper integrates trusted computing to bind cryptographic keys to trusted states, reducing the level of trust required from corporate and external administrators. This approach aims to mitigate the privacy and confidentiality risks often associated with corporate cloud computing.

Another significant contribution to cloud data security is presented byYong Wang and Ping Zhang (2017)** in their paper *"Enhance Big Data Security in Cloud Using Access Control"*. This work highlights the critical role of securing big data, which has become crucial for enterprises leveraging it for various applications such as customer targeting, fraud analytics, and anomaly detection. The paper emphasizes the challenges of securing big data frameworks like Hadoop, Hive, Presto, and Spark, due to their distributed nature and the complexities of monitoring access and data flows. As cloud adoption accelerates, ensuring the security of big data becomes increasingly complex, requiring robust access control mechanisms to prevent unauthorized or accidental data disclosure. Wang and Zhang's research underscores the need for effective access control strategies to safeguard sensitive information and maintain enterprise integrity amidst the evolving landscape of cloud computing.

III.EXISTING SYSTEM

Cloud computing is seen as an essential, low-maintenance way to share resources. More and more, moving the systems that manage the local information into cloud servers has become the standard procedure, clients being able to benefit of premium services whilst saving big money on the local infrastructures. Users that use cloud computing are no longer faced with the disadvantages of the problematic local solutions for storing and management of data. Using policy of encrypted data based on access control is the most common privacy method. This policy cab ensures privacy of data that represent sensitive information. The privacy based on access

control means to allow access to data only to authorized persons. The access mechanisms to the sensitive data have problems if they can be shared without strong privacy.

Disadvantages

1. Data is often in cloud or big data with shared access with third party, which makes it more vulnerable to attacks. Usually, moving data between sides can be risky on client privacy.

IV.PROPOSED SYSTEM

In our paper we are forwarding a case study that is built on the basis of three models: first model consists of the cloud's architecture, which will contain all the transactions for the other models; the second model is based on the concept of transactions' manager, who provides Keys, grand users, manages the queries and so forth; and finally, the last model is the one concerned with the clients, i.e. the staff that already has the right to use data in the cloud or analysis of big data. The cloud architecture is managed by providers of services. In addition, we consider that the case study is based on the assumption of zero trust between the three models. This situation is due to the fact that all transactions will be carried out by a third party and data movements through various levels of security. Among the tasks of the transactions' manager we might enumerate: user registration, generation of system parameters, user revocation, and the verification of the identity of data owners. The clients' model is a dynamic one, depending on the kind of transactions and data used.

Advantages

1. They proposed protecting from concerns of attacks on the data stored in the cloud using model segregation of the data. The data value in cloud gained during acquisition is separated in multi-location to support privacy of clients.
2. Access to data in cloud presents no risk since loading and using the data is allowed only to authenticated users and owners of data, with mapped manner to view the information set together.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

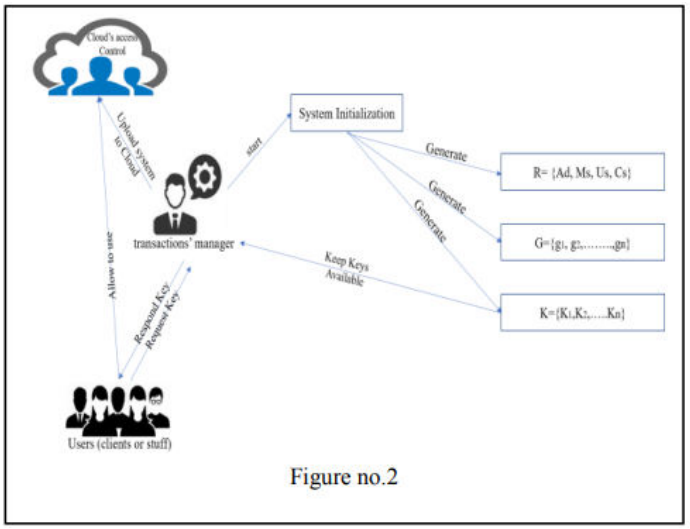


Figure no.2

Fig1: System Architecture

V.MODULES

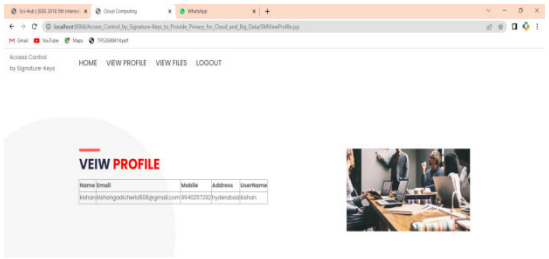
1. TRANSACTION MANAGER
2. ADMIN
3. SYSTEM MANAGER
4. CLIENT
5. CLOUD

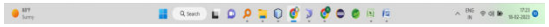
Module description

1. **CLIENT**
   Here client should register with our application after registration then client should login with the application after successful login he view profile, request keys and

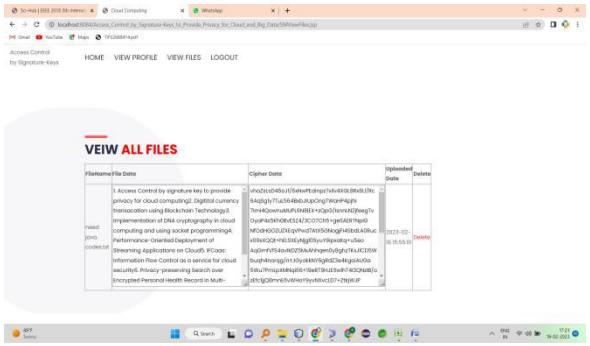
   view keys, new service register for cloud , user cloud services and logout.
2. **ADMIN**
   Here admin also should register with the application, here this admin role is assigned by the transaction manager, after that admin can login he can perform some operation such as view profile, view files and can have the change to delete and logout.
3. **SYSTEM MANAGER**
   Here manager also should register with the application, here this manager role is assigned by the transaction manager, after that manager can login he can perform some operation such as view profile, upload files and view files and logout.
4. **TRANSACTION MANAGER**
   Here manager is a module can directly login with the application after successful login he can perform some operations such as create role and view, create group and view, view all users, view key request, verify and assign group, view service users, view group members and can have the chance to exclude the group member also and logout.
5. **CLOUD**
   Here cloud can directly login with the application and after successful login he can perform some operation such as view all uploaded file in the cloud and logout

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

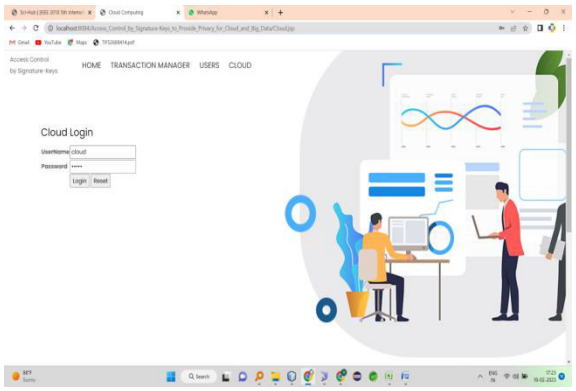




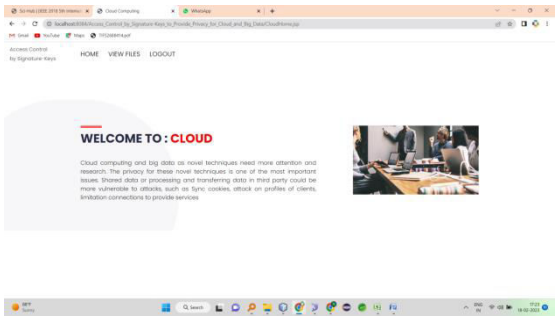
view all files and can delete



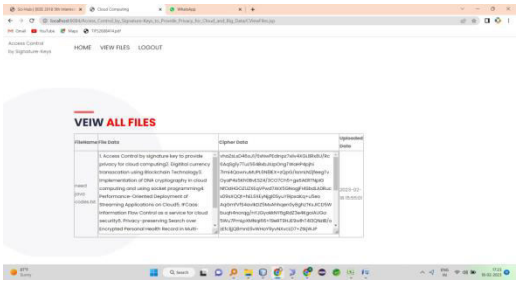
Cloud home



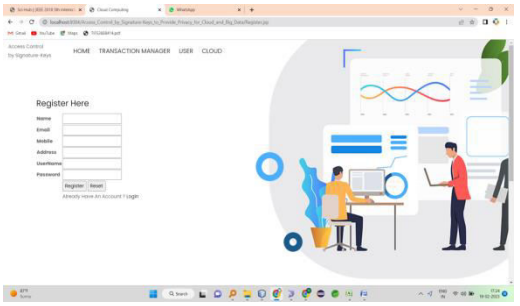
Cloud home



view files



Registration page



VI. CONCLUSION

Cloud computing and big data as novel techniques need more attention and research. The privacy for these novel techniques is one of the most important issues. Shared data or processing and transferring data in third party could be more vulnerable to attacks, such as Sync cookies, attack on profiles of clients, limitation connections to provide services, etc. [1]. Cloud computing implies a set of computers that are used together to provide different accounts and services. The benefits of using cloud computing in companies are cost reduction and time saving. Also, using shared services from cloud is easier than to building and developing own infrastructure. The providers of cloud computing focus to provides a flexible service, cost-effective IT infrastructure and secure environments for companies and organizations [4]. The variety of privacy models and whichever provides a guarantee to maintain cloud computing or big data privacy requires research and study to determine the best and

the most appropriate one to be applied in the future. In this paper, we reviewed methods of privacy and we focused on proposing a case study that is built on levels containing three models: cloud's architecture, transaction's manager and clients. Moreover, we consider that our case study is based on the premise of zero trust among the three models, therefore all the transactions take place with third-parties and the data movements are realized going through various levels of security. So, we implemented and exam our system's models which proved in-order to support privacy for three models. Also, was the result to protect data and change the base of our case study from zero- trust to trust for three models. we focus on the transactions' manager model because he represents the main model and we assume another two models in our research, which have already been built previously.

VII.REFERENCES

[1] Ulrich xzzzq , Benjamin Justus, Dennis Loehr,(2011), A Privacy Preserving System for Cloud Computing. International Conference on Computer and Information Technology .

[2] Jonathan Strickland,2017, "How Cloud Computing Works", HowStuffWorks.com. http://computer.howstuffworks.com/cloudcomputing/cloud-computing.htm. 2017

[3] Yong Wang , Ping Zhang ,(2017), Enhance Big Data Security in Cloud Using Access Control , Int'l Conf. on Advances in Big Data Analytics ,2017.

[4] Kire Jakimoski, (2016), Security Techniques for Data Protection in Cloud Computing, International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016), pp.49-56.

[5] Iynkaran Natgunanathan, Yong Xiang, Guang (2016) HUA, Song Guo, (2016), IEEE Access · January 2016, DOI: 109/ACCESS.2016.2558446.

[6] Micha_l Wrzeszcz, _Lukasz Opio_la, Konrad Zemek, Bartosz Kryza, _Lukasz Dutka, Renata S_lota, and Jacek,(2017), International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland

[7] Banks, David, John S. Erickson, and Michael Rhodes. (2009), "Toward cloud-based collaboration services." In Usenix Workshop HotCloud. 2009.

[8] Elham Abd Al Latif Al Badawi1 & Ahmed Kayed, (2015), SURVEY ON ENHANCING THE DATA SECURITY OF THE CLOUD COMPUTING ENVIRONMENT BY USING DATA SEGREGATION TECHNIQUE, IJRRAS 23 (2) - May 2015.

[9] R. Banyal, P. Jain, and V. Jain, 2013, Multi-factor authentication framework for loud computing in Fifth International Conference on Computational Intelligence, Modeling and Simmulation. Pp 105-110.

[10] H. Kim, and S. Timm, 2014, X.509 Authentication and Authorization in femi cloud. IEEE/ACM 7th International Conference on Utility and Cloud Computing. Pp 732-737.

Dr.AR.SIVAKUMARAN, has been working as a Associate Professor in Department of Information Technology, Malla Reddy Engineering College for Women, Secunderabad, Telangana, India, since 2019. He received his Doctorate Degree from Anna University, Chennai, Tamil Nadu. He received M.Tech(CSE)

Degree from Motilal Nehru National Institute of Technology (NIT), Allahabad, Uttar Pradesh. He has a Good Academic and Research Experience of more than 23 years. His current area of research includes Web Mining, AI, NLP, Deep Learning and Machine Learning. He has published many papers in Scopus, UGC Care List and reputed International Journals. He has five patent publications