ACCESS CONTROL BY SIGNATURE KEYS TO PROVIDE PRIVACY FOR CLOUD AND BIG DATA

1 Mr. R. MADHAVA REDDY, 2D. KAVITHA SRI, 3B. SHARATH, 4B. AJAY

1Assistant Professor, Department of AI&DS, Sri Indu College of Engineering and Technology-Hyderabad

234Under Graduate, Department of AI&DS, Sri Indu College of Engineering and Technology-Hyderabad

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.

Keywords: **Cloud and Big Data, Signature Key Controls**

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. 2

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 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. 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.

LITERATURE SURVEY

Cloud computing is changing the way that organizations manage their data, due to its robustness, low cost and ubiquitous nature. Privacy concerns arise whenever sensitive data is outsourced to the cloud. This paper introduces a cloud database storage architecture that prevents the local administrator as well as the cloud administrator to learn about the outsourced database content. Moreover, machine readable rights expressions are used in order to limit users of the database to a need-to-know basis. These limitations are not changeable by administrators after the database related application is launched, since a new role of rights editors is defined once an application is launched. Furthermore, trusted computing is applied to bind cryptographic key information to trusted states. By limiting the necessary trust in both corporate as well as external administrators and service providers, we counteract the often criticized privacy and confidentiality risks of corporate cloud computing.

Big data has become an essential requirement for enterprises looking to harness their business potential. The use cases for big data are endless and range from customer targeting and fraud analytics to anomaly detection and more. This data can be generated quickly from various sources such as users' browser and search history, credit card payments, mobile pinging of the nearest cell phone tower, etc. Given the volume of sensitive information being captured, any or accidental disclosure of or access to the data can have severe consequences for your enterprise, both in financial terms and in more intangible ways, such as the loss of brand recognition and users' trust.

In recent years, many highly scalable and complex processing *frameworks for big data* have emerged, such as Hadoop, Hive, Presto, and Spark. Securing these frameworks is very challenging because of their distributed nature, and involves many touchpoints, services, and operational processes. With accelerating cloud adoption, monitoring access and data flows for big data becomes even more complicated. 4

The IBM Security® Guardium® Insights data security platform allows any enterprise to quickly address their data security and compliance needs. Its robust capabilities help enterprises automate compliance policy enforcement and centralize data activity from multiple clouds. This enhances visibility to achieve a consolidated view of how critical data is being accessed and used across hybrid environments. Guardium Insights is designed to provide data security specialists with a centralized hub where they can retain monitoring data for compliance or analytic purposes for as long as they need to. With best- in-class features such as automated compliance, audit and reporting, and real-time monitoring, Guardium Insights can help users achieve a reduction in audit prep time. Guardium Insights can complement and enhance existing Guardium® Data Protection deployments or be installed on its own to help solve compliance and cloud data activity monitoring challenges.

As we approach the end of the first decade of the 21st century, we are witnessing a disruptive change in the provisioning of information technology: the advent of cloud computing. For most organizations, information technology is not a core competence. Until recently, their only option was to retain IT specialists on premise, but now alternatives from the likes of Google, Amazon and Salesforce.com are becoming increasingly viable. Accordingly, out-sourced IT is now an option for all sizes of company. This coincides with businesses seeking to operate efficiently in a global marketplace by outsourcing noncore competencies. As businesses choose to excel in a single area and partner for the rest, collaboration across organizational boundaries becomes a core part of product development. Traditional Enterprise Content Management (ECM) software has not kept up, leaving people collaborating via email—the lowest common denominator. In response to these trends, we envision a generation of cloud-based collaboration platforms emerging to address the needs of content-centered collaboration between businesses. millions of users.

SYSTEM ANALYSIS

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. **Key Distribution:** Distributing signature keys securely to authorized users or entities can be challenging. If not handled properly, it can lead to key exposure or unauthorized access. Implementing secure key distribution mechanisms is crucial

Human Error: Users may accidentally mishandle their signature keys, leading to access problems or security vulnerabilities. Training and user education are essential to mitigate this.

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.

ADVANTAGE OF PROPOSED SYSTEM

 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 only to authenticated users and owners of data, with mapped manner to view the information set together.

IMPLEMENTATION

MODULE DESCRIPTION

CLIENT

Here client should register with our application after registration then client should login with the application after successful login view profile, request keys and view keys, new service register for cloud, user cloud services and logout. The client module is essential in the interaction between users or applications and the cloud or big data system. In the context of access control using signature keys, the client module plays a significant role in securely communicating with the system. It is responsible for handling user authentication, encryption/decryption using signature keys, and ensuring that only authorized users can access the system or data. By incorporating access control using signature keys within the client module, organizations can strengthen the security of their cloud and big data systems. The client module helps in securely exchanging data, verifying user identities, and maintaining the confidentiality and integrity of information.

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. he admin module is a critical component in managing access control. within cloud and big data systems. In this context, the admin module is responsible for overseeing user permissions, roles, and access levels. It allows administrators to define and control who has access to what data and functions within the system.

By utilizing signature keys, the admin module can enforce secure access control policies based on the verification of these keys. Admin modules typically handle tasks such as user authentication, authorization, and user role management. They ensure that only authorized users with the correct signature keys can access specific data or perform certain actions within the system. This helps maintain data privacy, security, and integrity in cloud and big data environments. By integrating access control using signature keys with a robust admin module, organizations can establish a strong security framework to protect sensitive information and regulate access effectively.

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. . The system manager module plays a crucial role in overseeing the overall operation and functionality of the system. In the context of cloud and big data environments, the system manager module is responsible for managing resources, monitoring system performance, and ensuring the smooth operation of the entire system. When it comes to access control using signature keys, the system manager module can help enforce security policies, track system activity, and ensure that the access control mechanisms are functioning correctly. By integrating access control using signature keys with a robust system manager module, organizations can enhance the security and privacy of their cloud and big data systems. The system manager can help in maintaining the integrity of access control processes, detecting any anomalies, and responding to security incidents effectively.

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. let's talk about the transaction manager module. In the context of cloud and big data systems, the transaction manager plays a crucial role in ensuring the integrity and consistency of transactions. It oversees the execution of transactions, ensuring that they are processed correctly and in compliance with ACID (Atomicity, Consistency, Isolation, Durability) properties. 29

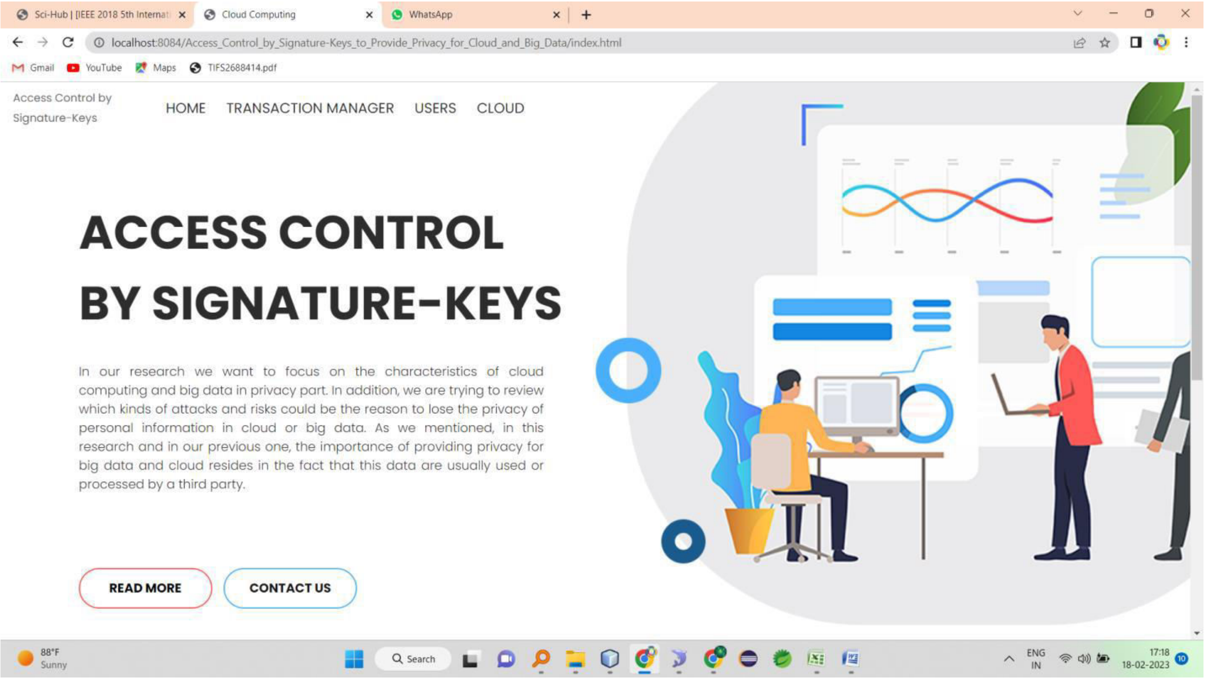
The transaction manager module coordinates the initiation, execution, and completion of transactions, handling issues such as concurrency control and recovery from failures. It helps maintain data integrity by ensuring that transactions are either fully completed or fully aborted, preventing partial updates that could lead to inconsistencies in the database.

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. The cloud module is a critical component that stores and processes data in cloud computing environments. When it comes to access control using signature keys in the cloud module, it helps ensure that data stored in the cloud is accessed securely and only by authorized users. Signature keys are used to authenticate users and validate their access permissions, enhancing data privacy and security in cloud environments. By implementing access control using signature keys in the cloud module, organizations can effectively manage and control access to sensitive data, reducing the risk of unauthorized access or data breaches. This approach helps maintain the confidentiality and integrity of data stored in the cloud, providing a secure environment for big data processing and storage.

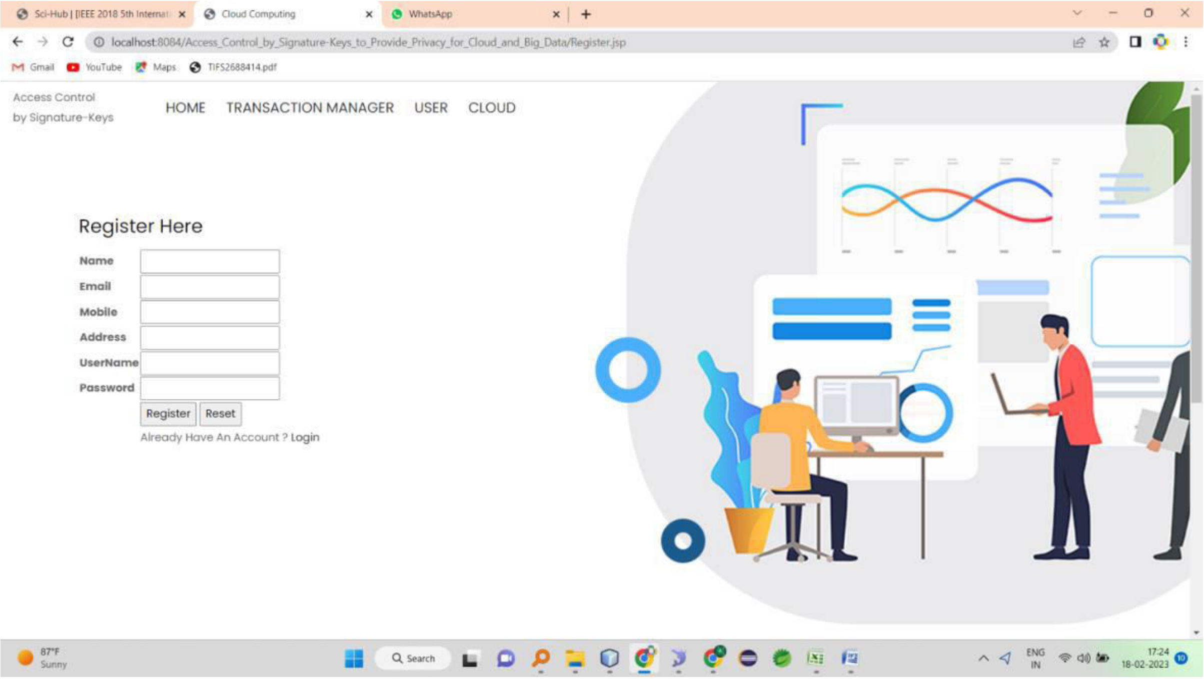
RESULTS

The term "Index" refers to the main or initial screen of an application or website that users encounter upon opening the application or accessing the website. The Index is essentially the starting point and often sets the tone for the rest of the user experience.


Sci-Hub | [IEEE 2018 5th Internati
Cloud Computing
WhatsApp
localhost:8084/Access_Control_by_Signature-Keys_to_Provide_Privacy_for_Cloud_and_Big_Data/index.html
Gmail
YouTube
Maps
TIFS2688414.pdf
Access Control by Signature-Keys
HOME
TRANSACTION MANAGER
USERS
CLOUD
READ MORE
CONTACT US
88°F Sunny
Search
ENG IN
17:18 18-02-2023

ACCESS CONTROL BY SIGNATURE-KEYS

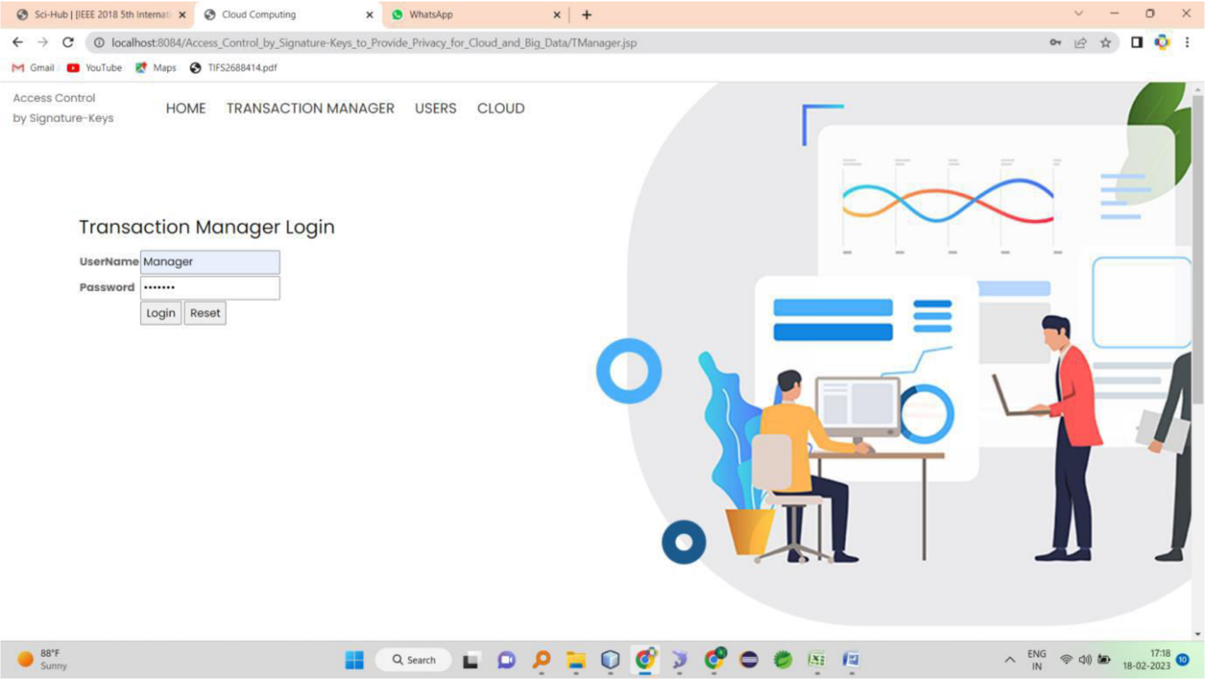
In our research we want to focus on the characteristics of cloud computing and big data in privacy part. In addition, we are trying to review which kinds of attacks and risks could be the reason to lose the privacy of personal information in cloud or big data. As we mentioned, in this research and in our previous one, the importance of providing privacy for big data and cloud resides in the fact that this data are usually used or processed by a third party.


Sci-Hub | [IEEE 2018 5th Internati
Cloud Computing
WhatsApp
localhost:8084/Access_Control_by_Signature-Keys_to_Provide_Privacy_for_Cloud_and_Big_Data/Register.jsp
Gmail
YouTube
Maps
TIFS2688414.pdf
Access Control by Signature-Keys
HOME
TRANSACTION MANAGER
USER
CLOUD
Register
Reset
87°F Sunny
Search
ENG IN
17:24 18-02-2023

Register Here

Name	
Email	
Mobile	
Address	
UserName	
Password	

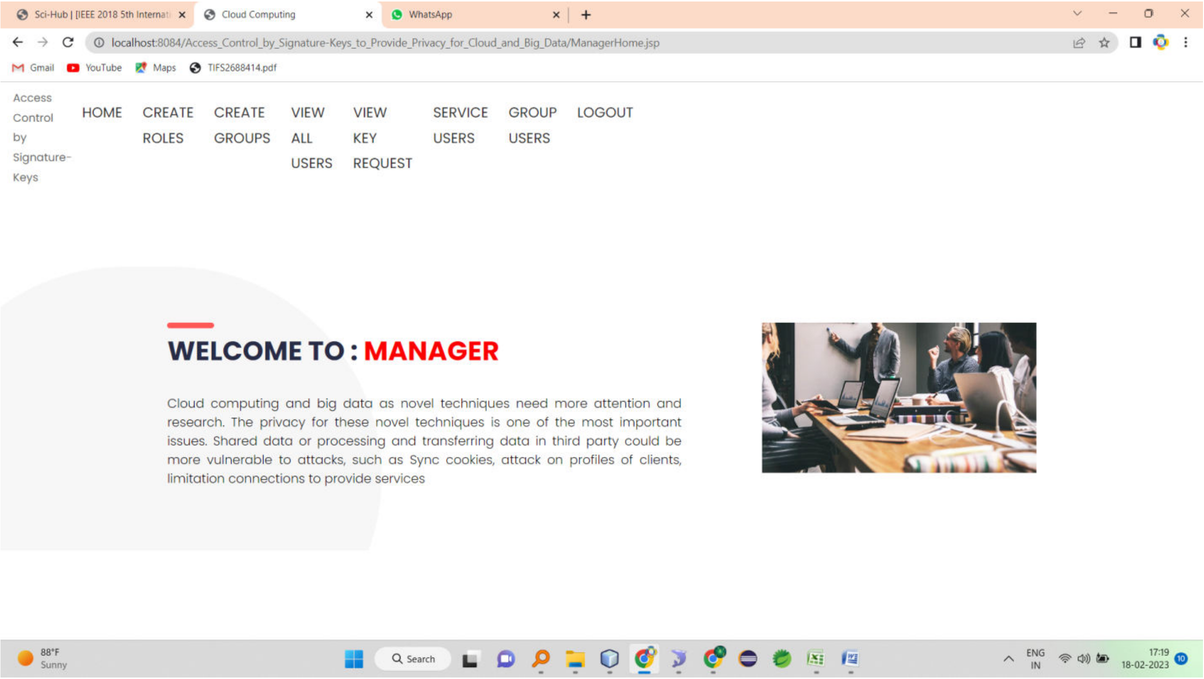
Already Have An Account ? Login


Sci-Hub | [IEEE 2018 5th Internati
Cloud Computing
WhatsApp
localhost:8084/Access_Control_by_Signature-Keys_to_Provide_Privacy_for_Cloud_and_Big_Data/TManager.jsp
Gmail
YouTube
Maps
TIFS2688414.pdf
Access Control by Signature-Keys
HOME
TRANSACTION MANAGER
USERS
CLOUD
Login
Reset
88°F Sunny
Search
ENG IN
17:18 18-02-2023

Transaction Manager Login

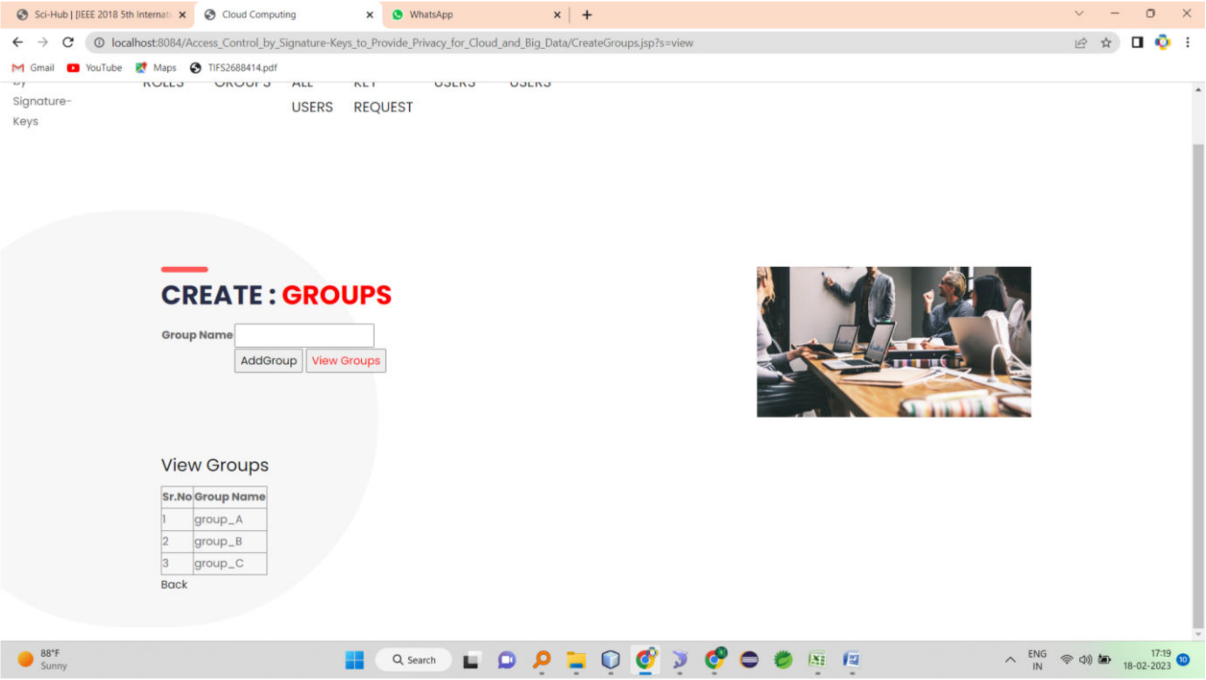
UserName Manager

Password •••••••



WELCOME TO : MANAGER

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


localhost:8084/Access_Control_by_Signature-Keys_to_Provide_Privacy_for_Cloud_and_Big_Data/CreateGroups.jsp?s=view
Signature-
Keys
ALL
USERS
KEY
REQUEST
AddGroup
View Groups
Back

CREATE : GROUPS

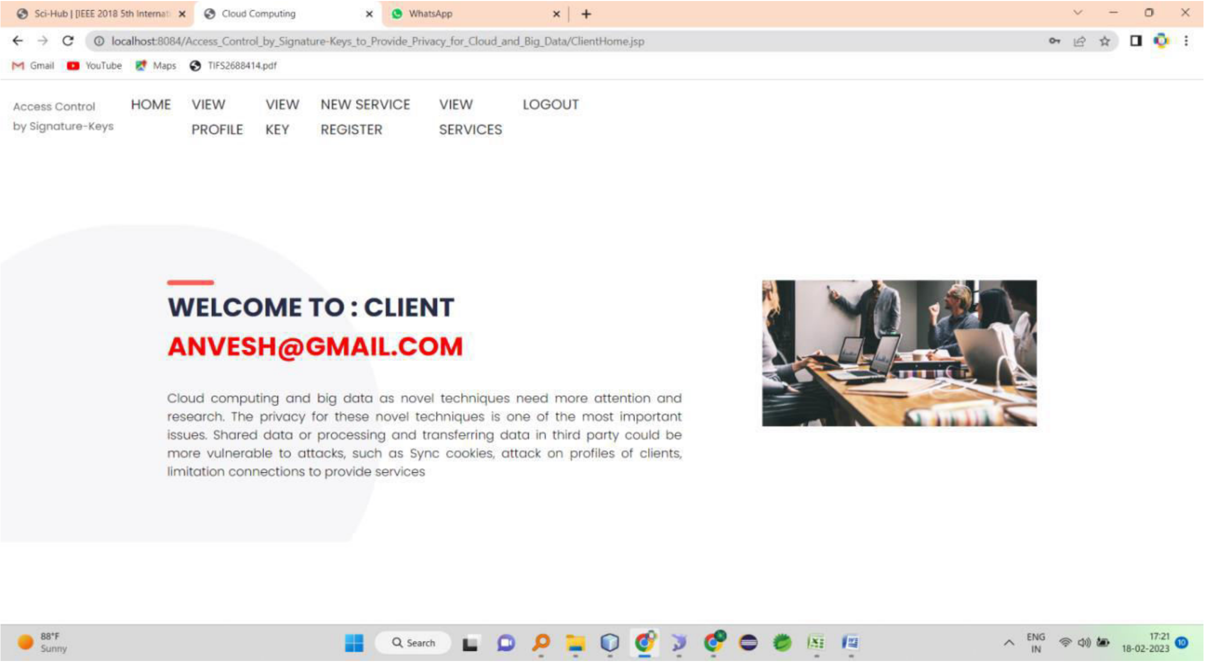
Group Name

View Groups

Sr.No	Group Name
1	group_A
2	group_B
3	group_C

VIEW ALL USERS AND ASSIGN ROLE

Administrators can easily access a comprehensive list of all users, review their details, and efficiently assign or modify roles as needed. This streamlined process enhances administrative control, ensuring that each user has the appropriate permissions and access levels.


localhost:8084/Access_Control_by_Signature-Keys_to_Provide_Privacy_for_Cloud_and_Big_Data/ClientHome.jsp
Access Control
by Signature-Keys
HOME
VIEW
PROFILE
VIEW
KEY
NEW SERVICE
REGISTER
VIEW
SERVICES
LOGOUT

WELCOME TO : CLIENT
ANVESH@GMAIL.COM

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

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.

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.

REFERENCES

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

[2] Jonathan Strickland,2017, "How Cloud Computing Works", HowStuffWorks.com.

[3] 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

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] Banks, David, John S. Erickson, and Michael Rhodes. (2009), "Toward cloudbased SSSScollaboration services." In Usenix Workshop HotCloud. 2009.