Access Control Based Efficient Hybrid Security Mechanisms For Cloud Storage

M.Gowrisanker [1], Kaviyarasan.M [2], Sarathi.M [3], Vasudevan.V [4]
[1]Assistant Professor, Dept of Computer Science
[2, 3, 4]Dept of Computer Science
[1, 2, 3, 4] Mahendra Institute of Engineering and Technology,Tamil Nadu, Namakkal DT – 637 503

Abstract- *The genuine purposes of this strategy a safe multi-proprietor data sharing arrangement. It derives that any customer in the social affair can securely give data to others by the untrusted cloud. This arrangement can support dynamic social occasions. Profitably, especially, new permitted customers can clearly unscramble data archives exchanged before their backing without coming to with data proprietors. Customer revocation can be successfully proficient through a novel foreswearing list without updating the puzzle Keys of whatever remains of the customers. The size and count overhead of encryption are steady and Independent with the amount of revoked customers. The present a safe and security ensuring access control to customers, which guarantee any part in a social event to anonymously utilize the cloud resource. Likewise, the veritable identities of data proprietors can be revealed by the get-together executive when open deliberation happen. We give careful security examination, and perform expansive generations to show the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated figuring gives a traditionalist and gainful response for sharing social event resource among cloud customers. Shockingly, sharing data in a multi-proprietor way while shielding data and identity security from an untrusted cloud is still a testing issue, in light of the constant change of the enlistment*

I. INTRODUCTION

Objective

The genuine purposes of this strategy a safe multi-proprietor data sharing arrangement. It derives that any customer in the social affair can securely give data to others by the untrusted cloud. This arrangement can support dynamic social occasions. Profitably, especially, new permitted customers can clearly unscramble data archives exchanged before their backing without coming to with data proprietors. Customer revocation can be successfully proficient through a novel foreswearing list without updating the puzzle Keys of whatever remains of the customers. The size and count overhead of encryption are steady and Independent with the number of revoked customers. We present a safe and security ensuring access control to customers, which guarantee any part in a social event to anonymously utilize the cloud resource. Likewise, the veritable identities of data proprietors can be revealed by the get-together executive when open deliberation happen. We give careful security examination, and perform expansive generations to show the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated figuring gives a traditionalist and gainful response for sharing social event resource among cloud customers. Shockingly, sharing data in a multi-proprietor way while shielding data and identity security from an untrusted cloud is still a testing issue, in light of the constant change of the enlistment.

II. CLOUD OPERATIONS

The transition from onsite servers to a public cloud provider requires a significant paradigm shift. Due to the rising popularity of cloud computing, it's a change many organizations are in the process of adopting. Using CloudOps in conjunction with DevOps offers your operation more speed, scalability, and productivity. Facilitate your team's progression to CloudOps by implementing the following best practices.

Enable Agility

It's essential that your security or governance team is fully onboard with every aspect of cloud computing. If teams fail to work together and make usage more difficult, the end result will be less transparency and a lack of overall cohesiveness. Don't create more restrictions; instead, clearly define and implement necessary guidelines.

III. CLOUD SERVICE

The term "cloud services" refers to a wide range of services delivered on demand to companies and customers over the internet. These services are designed to provide easy, affordable access to applications and resources, without the need for internal infrastructure or hardware. From checking email to collaborating on documents, most employees use

cloud services throughout the workday, Cloud deployment describes the way a cloud platform is implemented, how it's hosted, and who has access to it. All cloud computing deployments operate on the same principle by virtualizing the computing power of servers into segmented, software-driven applications that provide processing and storage capabilities.

Public Cloud

Some public cloud examples include those offered by Amazon, Microsoft, or Google. These companies provide both services and infrastructure, which are shared by all customers. Public clouds typically have massive amounts of available space, which translates into easy scalability. A public cloud is often recommended for software development and collaborative projects. Companies can design their applications to be portable, so that a project that's tested in the public cloud can be moved to the private cloud for production. Most cloud providers package their computing resources as part of a service. Public cloud examples range from access to a completely virtualized infrastructure that provides little more than raw processing power and storage (Infrastructure as a Service, or IaaS) to specialized software programs that are easy to implement and use (Software as a Service, or SaaS). 5 The great advantage of a public cloud is its versatility and "pay as you go" structure that allows customers to provision more capacity on demand. On the downside, the essential infrastructure and operating system of the public cloud remain under full control of the cloud provider. Customers may continue to use the platform under the terms and conditions laid out by the provider, but they may have difficulty repatriating their assets if they want to change providers. Should the provider go out of business or make significant changes to the platform, customers could be forced to make significant infrastructure changes on short notice. There's also the risk of an unpatched security vulnerability in the cloud architecture exposing customers to risk.

Private Cloud

Private clouds usually reside behind a firewall and are utilized by a single organization. A completely on-premises cloud may be the preferred solution for businesses with very tight regulatory requirements, though private clouds implemented through a colocation provider are gaining in popularity. Authorized users can access, utilize, and store data in the private cloud from anywhere, just like they could with a public cloud. The difference is that no one else can access or utilize those computing resources. Private cloud solutions offer both security and control, but these benefits come at a cost. The company that owns the cloud is responsible for both software and infrastructure, making this a less economical model than the public cloud. The additional control offered by a private cloud makes it easier to restrict access to valuable assets and ensures that a company will be able to move its data and applications where it wants, whenever it wants. Furthermore, since the private cloud isn't controlled by an outside vendor, there's no risk of sudden changes disrupting the company's entire infrastructure. A private cloud solution will also not be affected by a public cloud provider's system downtime. But private clouds also lack the versatility of public clouds. They can only be expanded by adding more physical compute and storage capacity, making it difficult to scale operations quickly should the business need arise.

Hybrid Cloud

Hybrid clouds combine public clouds with private clouds. They are designed to allow the two platforms to interact seamlessly, with data and applications moving smoothly from one to the other.The primary advantage of a hybrid cloud model is its ability to provide the scalable computing power of a public cloud with the security and control of a private cloud. Data can be stored safely behind the firewalls and encryption protocols of the private cloud, then moved securely into a public cloud environment when needed. This is especially helpful in the age of big data analytics, when industries like healthcare must adhere to strict data privacy regulations while also using sophisticated algorithms powered by artificial intelligence (AI) to derive actionable insights from huge masses of unstructured data. There are two commonly used types of hybrid cloud architecture. Cloud bursting uses a private cloud as its primary cloud, storing data and housing proprietary applications in a secure environment. When service demands increase, however, the private cloud's infrastructure may not have the capacity to keep up. That's where the public cloud comes in. A cloud bursting model uses the public cloud's computing resources to supplement the private cloud, allowing the company to handle increased traffic without having to purchase new servers or other infrastructure. The second type of hybrid cloud model also runs most applications and houses data in a private cloud environment, but outsources non-critical applications to a public cloud provider. This arrangement is common for organizations that need to access specialized development tools (like Adobe Creative Cloud), basic productivity software (like Microsoft Office 365), or CRM platforms (like Salesforce). Multi-cloud architecture is often deployed here, incorporating multiple cloud service providers to meet a variety of unique organizational needs.

Community Cloud

Although not as commonly used as the other three models, community clouds are a collaborative, multi-tenant platform used by several distinct organizations to share the same applications. The users are typically operating within the same industry or field and share common concerns in terms of security, compliance, and performance. 7 In essence, a community cloud is a private cloud that functions much like a public cloud. The platform itself is managed privately, either in a data centre or on-premises. Authorized users are then segmented within that environment. These deployments are commonly used by government agencies, healthcare organizations, financial services firms, and other professional communities.

IV. SYSTEM ANALYSIS

EXISTING SYSTEM

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

DRAWBACKS:

1. Only hash functions are used for a node to derive a descendant’s key from its own key.

2. The space complexity of the public information is the same as that of storing the hierarchy.

3. The private information at a class consists of a single key associated with that class.

4. It is no flexible hierarchies.

5. Low efficiency.

V. PROPOSED SYSTEM

We propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyes the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

ADVANTAGES

- We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
- We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

SOFTWARE ENVIRONMENTS

SOFTWARE DESCRIPTION

FRONT END

Java The JAVA language was created by James Gosling in June 1991 for use in a set top box project. The language was initially called Oak, after an oak tree that stood outside Gosling's office - and also went by the name Green - and ended up later being renamed to Java, from a list of random words. Gosling's goals were to implement a virtual machine and a language that had a familiar C/C++ style of notation. The first public implementation was Java 1.0 in 1995. It promised "Write Once, Run Anywhere” (WORA), providing no-cost runtimes on popular platforms. It was fairly secure and its security was configurable, allowing network and file access to be restricted. Major web browsers soon incorporated the ability to run secure Java applets within web pages. Java quickly became popular. With the advent of Java 2, new versions had multiple configurations built for different types of platforms. For example, J2EE was for enterprise applications and the greatly stripped down version J2ME was for mobile applications. J2SE was the designation for the Standard Edition. In 2006, for marketing purposes, new J2 versions were renamed Java EE, Java ME, and Java SE, respectively. In 1997, Sun Microsystems approached the ISO/IEC JTC1 standards body and later the Ecma

International to formalize Java, but it soon withdrew from the process. Java remains a standard that is controlled through the Java Community Process. At one time, Sun made most of its Java implementations available without charge although they were proprietary software. Sun's revenue from Java was generated by the selling of licenses for specialized products such as the Java Enterprise System. Sun distinguishes between its Software Development Kit (SDK) and Runtime Environment (JRE)which is a subset of the SDK, the primary distinction being that in the JRE, the compiler, utility programs, and many necessary header files are not present.

Primary Goals:

There were five primary goals in the creation of the Java language:

- It should use the object-oriented programming methodology.
- It should allow the same program to be executed on multiple operating systems.
- It should contain built-in support for using computer networks.
- It should be designed to execute code from remote sources securely.
- It should be easy to use by selecting what were considered the good parts.

VI. MODULE DESCRIPTION

1. User Registration
2. User Revocation
3. File Uploading and Deletion
4. File Access and Traceability

1. User Registration

The registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.
Registration

2. User Revocation

User revocation is performed by the group manager via a public available. Revocation list, based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. Group manger update the revocation list each day even no user has being revoked in the day. In other words, the others can verify the freshness of the revocation list from the contained current date.

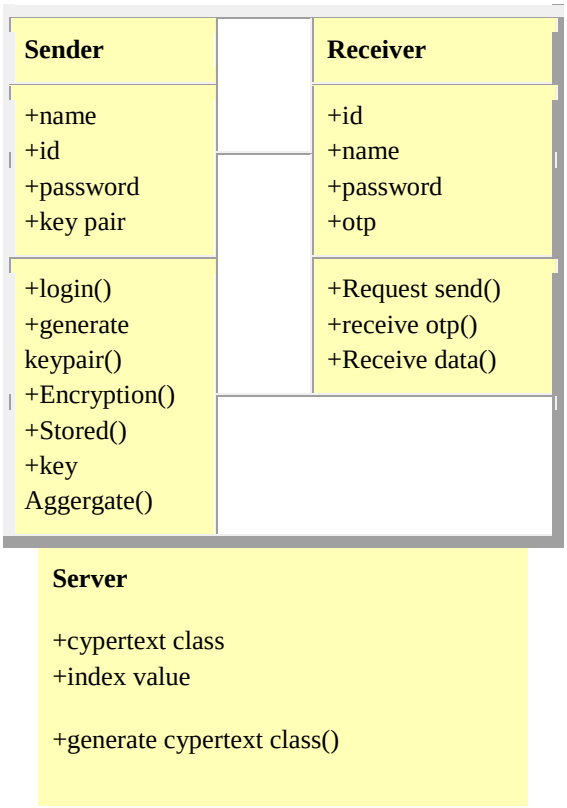
3. File Uploading and Deletion

To store and share a data file in the cloud, a group member performs to getting the revocation list from the cloud. In this step, the member sends the group identity ID group as a request to the cloud.Verifying the validity of the received revocation list. File stored in the cloud can be deleted by either the group manager or the data owner.

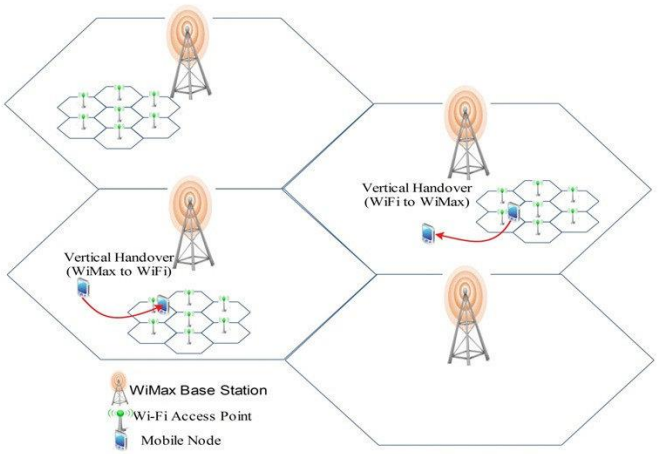
4. File Access and Traceability

To access the cloud, a user needs to compute a group signature for his/her authentication. The employed group signature scheme can be regarded as a variant of the short group signature which inherits the inherent enforceability property, anonymous authentication, and tracking capability. When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner.

DIAGRAM:



ACTIVITY DIAGRAM



SYSTEM TESTING

After the source code has been completed, documented as related data structures. Completed the project has to undergo testing and validation where there is subtitle and definite attempt to get errors.

The project developer treads lightly, designing and execution test that will demonstrates that the program works rather than uncovering errors, unfortunately errors will be present and if the project developer doesn't find them, the user will find out.

The project developer is always responsible for testing the individual units i.e. modules of the program. In many cases developer also conducts integration testing i.e. the testing step that leads to the construction of the complete program structure.

This project has undergone the following testing procedures to ensure its correctness

1.Unit Testing
2.Integration Testing
3.Valitation Testing

VII. CONCLUSION

The data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

VIII. FUTURE ENHANCEMENT

In Our future work will be how to avoid this type of re-computation introduced by dynamic groups while still preserving identity privacy from the public verifier during the process of public auditing on shared data.

REFERENCES

[1] Above the Clouds: A View of Cloud Computing Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia UC Berkeley Reliable Adaptive Distributed systems Laboratory (RAD Lab)

[2] A Survey of Cryptography Cloud Storage Techniques Nidal Hassan Hussein1, Ahmed Khalid2, Khalid Khanfar3 1 PhD. Program in Computer Science, Sudan University of Science and Technology, Sudan 2 Department of Computer Science, Community College, Najran University, Najran, KSA 3 Head of Information Security Department at Naif Arab University for Security, Saudi Arabia

[3] SiRiUS: Securing Remote Untrusted Storage Eu-Jin Goh, Hovav Shacham†, Nagendra Modadugu, Dan Boneh,Stanford University

[4] Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,Giuseppe Ateniese† Kevin Fu‡ Matthew Green† Susan Hohenberger.

[5] Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, Dept. of ECE, Worcester Polytechnic Institute, Email: {yscheng, wjlou}@ece.wpi.edu Dept. of ECE, Illinois Institute of Technology, Email: {cong, kren}@ece.iit.edu

[6] M. Abd-El-Malek, W. V. Courtright II, C. Cranor, G. R. Ganger, J.Hendricks, A. J. Klosterman, M. P. Mesnier, M. Prasad, B. Salmon,R. R. Sambasivan, S. Sinnamohideen, J. D. Strunk, E. Thereska,M. Wachs, and J. J. Wylie, "Ursa minor: Versatile cluster-basedstorage," in Proc. 4th USENIX Conf. File Storage Technol., Dec. 2005,pp. 59–72.

[7] C. Adams, "The simple public-key GSS-API mechanism (SPKM),"Internet Eng. Task Force (IETF), RFC 2025, Oct. 1996.

[8] Amazon simple storage service (Amazon S3) [Online]. Available: http://aws.amazon.com/s3/, 2014.

[9] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in Proc. 19th Int. Conf. Theory Appl. Cryptographic Techn., May 2000, pp. 139–155.

[10] White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes Jianting Ning, Xiaolei Dong, Zhenfu Cao, Senior Member, IEEE, Lifei Wei, and Xiaodong Lin, Senior Member, IEEE