Authentication key generator for data sharing on cloud by KAC Method

Abstract

With the help of a sizable quantity of virtual storage, cloud computing provides services through the Internet on demand. The primary benefit of cloud computing is that it relieves users of the need to invest in pricey computer equipment. Lower expenses are related with infrastructure. Researchers are looking at new, relevant technologies as a result of recent breakthroughs in cloud computing and other sectors. Due to its accessibility and scalability for computer operations, both private users and companies upload their software, data, and services into the cloud storage. While switching from local to remote computing provides advantages, there are also a few security issues and difficulties for both the supplier and the customer. There are many cloud services offered by reputable third parties, which is raising security concerns. The cloud service provider offers its services over the Internet and makes use of numerous online technologies, which raises fresh security concerns. Online data interchange for increased productivity and efficiency is one of today's most significant requirements. Owners of this data can keep and distribute the info online. This study aims to provide a secure key for online data sharing for users that includes cloud computing technologies and crypto algorithm principles. Data owners would ideally like to keep their data/files online in an encrypted way, delegate decryption rights for some of these to users, and maintain the ability to withdraw access at any moment.

Keywords—cloud protection, Framework for cloud computing, security issues, threats, and attacks

INTRODUCTION

With the recent emergence of cloud computing, countless applications that span international boundaries and include millions of users have seen their ability to share data stretched to the limit. Today, governments and businesses view data sharing as a crucial instrument for increased efficiency. Social networking, healthcare, and education have all been transformed through cloud computing. The ability of cloud computing to enable worldwide data sharing and interchange amongst various users without the hassles of manual data transfers and the creation of redundant or obsolete documents may be its most exciting use case. Social networking sites have made the globe more interconnected by utilizing the cloud to enable the sharing of text and multimedia. Cloud platforms frequently feature collaborative tools, which are very well-liked since they increase productivity and effort synchronization. The result of cloud computing has spread all over to the healthcare industry as well, with mobile applications enabling remote patient monitoring. In summary, cloud computing is drastically altering many facets of our existence. Despite all of its benefits, the cloud is vulnerable to security and privacy breaches, which pose a serious obstacle to its widespread adoption as the main method of data sharing in today's society. In a poll conducted by [1] cloud customers ranked security as their top difficulty, with 75% of people concerned about the security of their vital IT and business systems. Unknown service providers should also be explored, notwithstanding the predominance of security concerns posed by outside actors. It is difficult to ensure cloud security and privacy since internet data is virtually always stored in shared environments. (for example, many virtual computers running on the same physical device). When addressing data privacy and cloud security, it is critical to establish the requirements that a data sharing service must follow in order to be considered secure.

LITERATURE SURVEY

1) Spice-easy privacy-preserving identity management in the cloud Sherman SM Yi-
Authors: Jun He and Chow
Identity security and privacy have been listed as one of the top seven threats to cloud security. A few identity management solutions have recently been released in an attempt to address these concerns. All of these, however, fall short of the necessary characteristics. Unlinkability, in particular, ensures that no cloud service provider (CSP) may link the transactions of the same user, even if they collude. Delegatable authentication, on the other hand, is limited to cloud platforms, where a group of CSPs may collaborate to provide a packaged service, with one serving as the source provider who interacts with clients and handles authentication while the others remain invisible to them. It should be noted that CSPs may use various authentication methods that depend on various parameters. Also, each CSP is restricted to just seeing the properties that it is interested in. In addition to other desirable qualities, SPICE, the first digital identity management system, is presented in this work. Our method is unusual because it combines and takes use of two group signatures, allowing us to randomise the signature, making it appear new for each usage while concealing portions of the messages that are irrelevant to the CSP. Due to its effectiveness and simplicity, our technology is very suited to cloud-based applications.

2) Public auditing for secure cloud storage while protecting privacy
Authors: Cong Wang And Sherman S.-M. Chow
Users that use cloud storage can save their data remotely and utilise top-notch on-demand apps and services from a pool of shared reconfigurable computing resources without worrying about maintaining and storing their data locally. Protecting the integrity of the outsourced data in the cloud is a difficult problem, especially for users with low computer power, because users no longer physically possess the outsourced data. Also, users should be able to use cloud storage as if it were local without having to worry about verifying its integrity. As consumers can use a third-party auditor (TPA) to confirm the accuracy of outsourced data and feel secure, it is critical to offer public auditability for cloud storage. To deploy a TPA properly, the auditing process should not introduce any additional dangers to the privacy of user data or raise the user's online workload. We present a private public auditing mechanism for a secure cloud storage system in this study. We further broaden our conclusion so that the TPA may efficiently conduct audits for several customers at once. The suggested techniques are provably secure and extremely effective, according to a thorough investigation of security and performance. Our initial test, carried out on an Amazon EC2 instance, further confirms the design's quick performance.

3) Dynamic, secure, and provenance-based cloud storage
Cheng-Kang Chu and Sherman SM Chow are the authors.
One issue with employing cloud storage is the need for sensitive data to remain private to servers that are not under the data owners' control. Another difficulty is that while sharing or viewing the data, the user might desire to remain anonymous (such as in Web 2.0 applications). Cloud storage necessitates a fine-grained (one can specify who can access which classes of his or her encrypted files), dynamic (the total number of users is not fixed in the setup, and any new user can decrypt previously encrypted messages), scalable (space requirement does not depend on the number of decryptors), accountable (anonymity can be revoked if necessary), and secure confidential data sharing mechanism. (trust level is minimized). This research addresses the issue of creating a safe cloud storage system that supports dynamic users and data origin. Because it is built on certain constructs, the prior system does not provide all of the aforementioned desirable characteristics. The changeable user is not allowed, which is extremely important. We investigate the various benefits that private cryptographic verification and encryption methods provide. We then put our theory into practice by employing identity-based broadcast encryption with constant size ciphertexts and private keys, as well as verifier-local reversible group signing. To put our idea into practice, we create formal security assurances against adaptive chosen-ciphertext decryption and update attacks and outfit broadcast encryption with the possibility of dynamic ciphertext update.

4) For flexible data exchange in cloud storage, a key-aggregate cryptosystem

Authors include Cheng-Kang Chu and Sherman SM Chow.

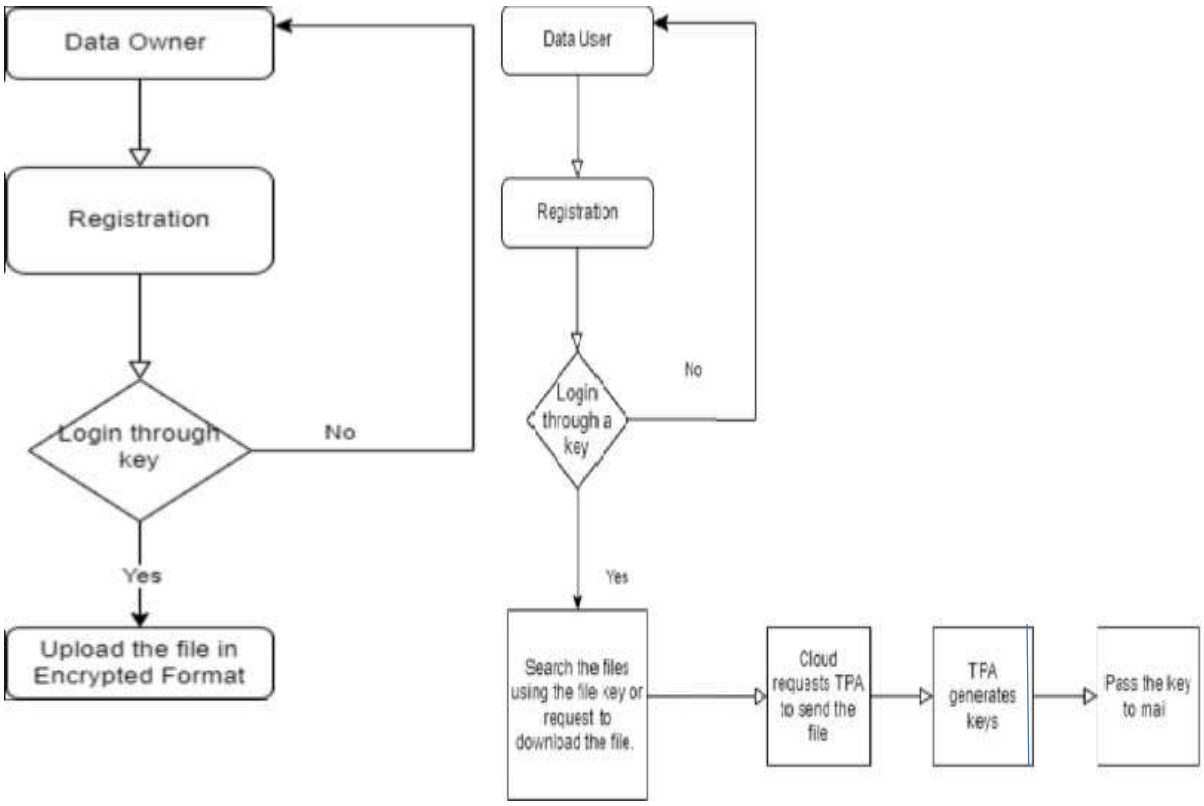
Data sharing is a critical aspect of online storage. In this piece, we show how to exchange data with others via cloud storage in an adaptable, secure, and efficient way. We explore innovative public-key cryptosystems that produce constant-size ciphertexts, making it simple to delegate decryption keys for any group of ciphertexts. The peculiarity is that any group of hidden keys can be combined into a single key while retaining all of the power of the individual keys. In other words, the proprietor of the secret key can share an aggregate key of fixed size for an adaptable cypher text set in cloud storage, but the other encrypted files outside of the set remain private. This small aggregate secret can be communicated to Others can be readily stored on a smart card with a tiny quantity of safe storage. We provide a rigorous security study of our systems in the standard format. We also talk about potential applications for our technologies. Previously undisclosed patient-controlled public-key encryption for flexible ordering is provided by our methods.

5) Short ciphertexts and private keys provide collusion-resistant broadcast encryption

Dan Boneh and Craig Gentry are the author

Two novel stateless recipient public key broadcast encryption methods are presented. Both techniques are totally safe from all conspirators. The first construction's ciphertexts and private keys are of constant size for each subgroup of recipients. (just two group elements). With this method, the size of the public key is proportional to the overall number of receivers. Our second approach is a refinement of the first, offering a trade-off between ciphertext size and public key size. For example, for any subgroup of recipients, we can design a collusion-resistant broadcast system for n users with ciphertexts and public keys of size O.(N). We go over a few of these technologies' applications.

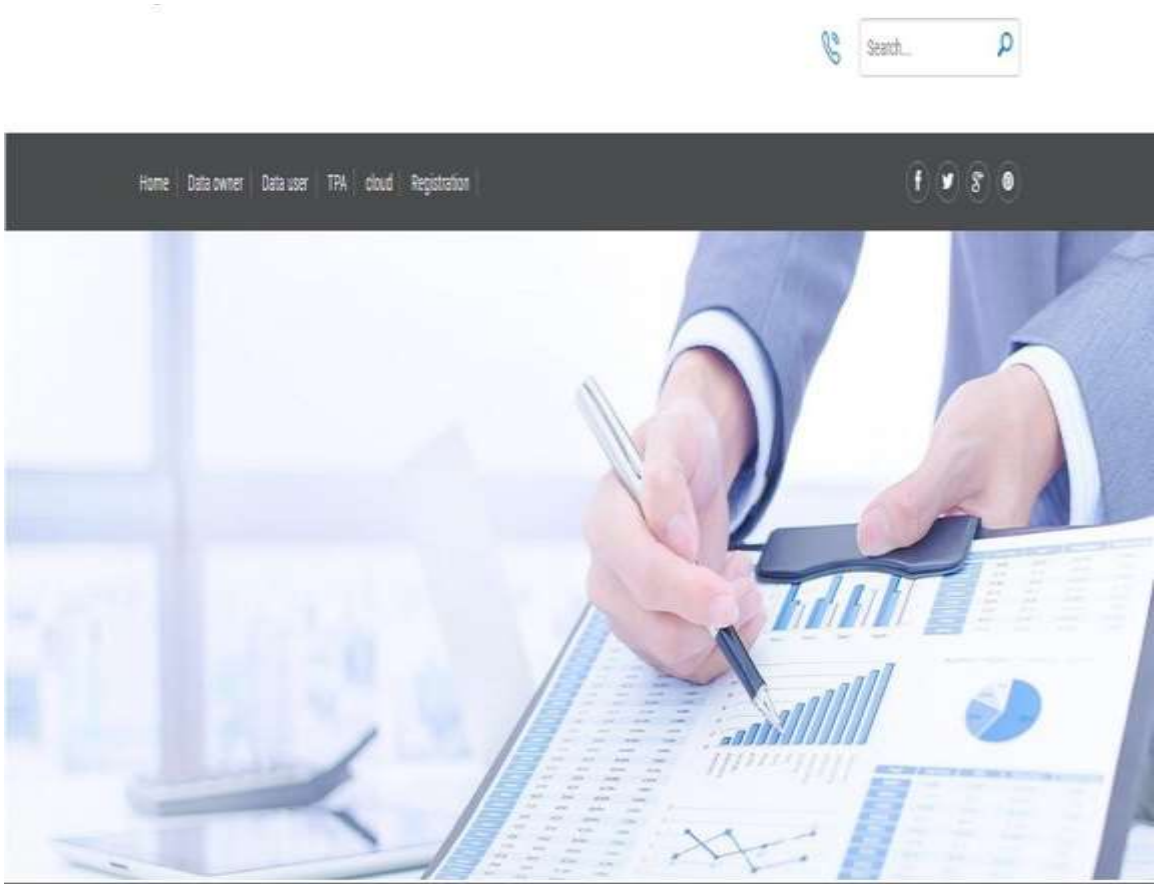
METHODOLOGY



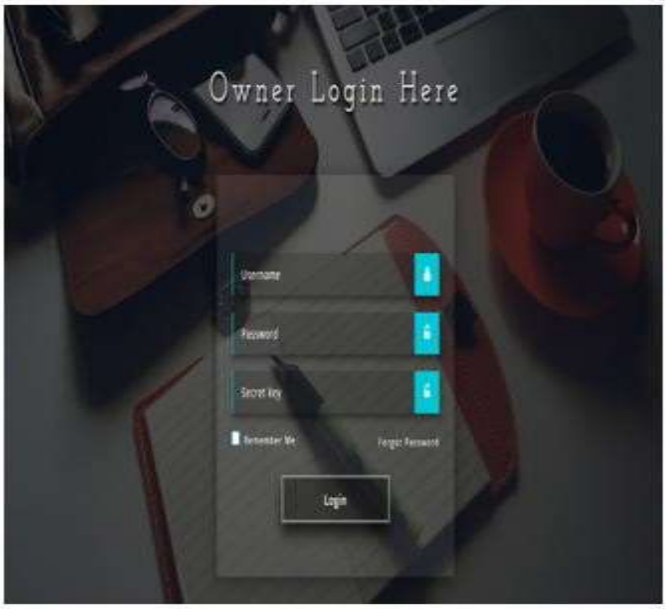
- **Data Owner:**
  The data owner uploads their information in an encrypted manner to the cloud. People can check in using the passcode they received in the mail.
- **Encryption of the data:**
  The data will be encrypted into the binary format. The owner will upload the encrypted data into the cloud so that the other people can't read the data so easily.
- **Data User:**
  Data user can search uploaded files by using file key.Data user also can login only using secrete key sent by cloud.user can download requested files from cloud by using third party generated private and aggregate keys.
- **Cloud:**
  Cloud can view user's file request.It request third party to send corresponding file to the user.It will store the data. The thiparty will generated the key to the users mail account.we can see all the file details.

The login of the user and the owner is done by using the secret keys generated by the mail.

RESULTS



This is the homepage for this site where there is an access for registration ,cloud login ,oner and user login etc.

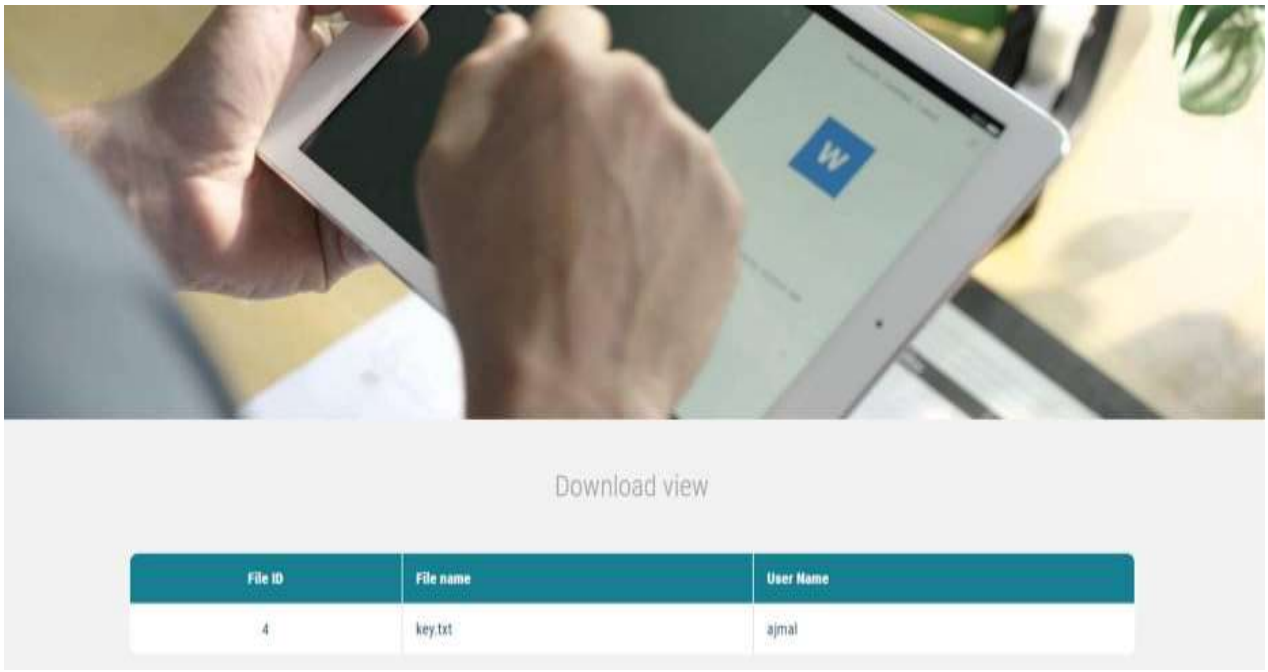


These are the loginpages of the owner and user.Here the owner and user can login only when h enter the secret key which is generated by the mail.The generation of the key will be done when we update the owner activation.

These are the TPA login page and cloud login page. In cloud page we will get the owner and user details by updating the active status we will be getting the secret key to the mail. By using this owner and user can login to their pages. Using TPA we can get the aggregate key and private key.

This is the owner page in this owner can upload the file which is in encrypted format.

This is the registration page where the data ownwer and user can register using this form.so that we can get the owner details and the user details.



These are the download details when the user downloaded the file.

Conclusion

Cloud computing include rapid system implementation, low costs, abundant storage, and simple system access from anywhere at any time As a result, cloud computing is becoming more and more apparent in recent technical developments and a widely utilised computer environment everywhere. Several security and privacy issues make it difficult to use cloud computing. The security weaknesses, dangers, and assaults that the cloud already has should be known to all users. If businesses are aware of security threats and attacks, they can adopt the cloud more swiftly.. Utilizing both traditional and cutting-edge techniques and technology, cloud computing. Multiple clouds can be produced using this innovative technique. Particular security concerns utilise the same resources physically located at the cloud from several places to virtualization and multi-tenancy features. The security of the system may be hampered by improperly segregated VMs. By generating the keys, we can improve online security and reduce dangers and attacks. We proposed a successfully implementable variant of the basic key-aggregate cryptosystem (KAC) with minimal overhead ciphertexts and aggregate keys using asymmetric bilinear pairings. Our design provides an efficient answer for a variety of cloud-based data sharing apps, including collaborative data sharing, product license distribution, and medical data sharing. We have proven that our structure is fully collusion resistant and semantically secure against a non-adaptive opponent under acceptable security assumptions. Following that, we demonstrated how this design could be modified to achieve CCA-safe building. To the best of our knowledge, this is the first CCA safe KAC design to be disclosed in the cryptographic literature. In a practical data sharing situation, the KAC architecture can be successfully extended and modified to safely disseminate the aggregate key across several data consumers. This provides creators with an important path toward developing a scalable, fully public-key-based online data-sharing system for widespread cloud implementation. We generated simulation findings to validate the requirements for our scheme's spatial and temporal complexity. The results indicate that KAC with aggregate key broadcast outperforms other existing safe data sharing methods in terms of speed and scaling.