KEY AGGREGATE SEARCHABLE ENCRYPTION FOR GROUP DATA SHARING VIA CLOUD STORAGE

G.Gnana kumar

R.KALPANA
B.E CSE
JEI MATHAAJEE COLLEGE OF ENGINEERING
KANCHIPURAM

M.MATRINA
B.E CSE
JEI MATHAAJ EE COLLEGE OF ENGINEERING
KANCHIPURAM

ABSTRACT: Cloud storage user to store the data and enjoy high quality application and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Data sharing is an important functionality in cloud storage. In this paper, we propose a Key Aggregate Cryptosystem is to show how to securely, efficiently, and flexibly share data with others in cloud storage. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. A constant size and more efficient text delegation for decryption rights for key set of cipher text are possible by using a new public key cryptosystem The innovation is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the key being secret key holder can realize cloud storage flexible choices to constant size aggregate key but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. Enabling the cloud storage for public auditability is for critical importance user can restore third party auditor(TPA)To securely introduce an effective TPA, the auditing process should bring in new vulnerabilities towards user data privacy, and introduce no additional online burden to user TPA can perform audits to multiple user both working the users simultaneously and efficiently .The proposed schemes are provably secure and highly efficient and then its shown by extensive security and performance analysis requirements are needed:

The shares must be masked during secret reconstruction phase.

Recovery of a secret must not jeopardize the secrecy of the other unrecovered secrets.

For a multi-secret sharing scheme to be multi-stage, the participants

1 INTRODUCTION

Secret sharing schemes are used as a tool in many cryptographic protocols including revocable electronic cash [1], electronic voting [2], cloud computing [3] and key management in sensor networks [4]. A secret sharing scheme (SSS) allows one to share a secret among a set P of parties, called participants. The participants are assigned different values called shares and only certain authorized subsets of them can recover the secret using these shares. The collection of the authorized subsets of participants is called the access structure and denoted by . In an SSS, we intend that any subset in can reconstruct the secret, while those not in cannot recover any information about the secret.

A secret sharing scheme was independently 1979[5][6] threshold access was introduced by Blakely and Shamir consists of all subsets schemes P including at least t participants. Many other secret sharing schemes have been proposed since then [7], [8]. Some new features have been added to secret sharing schemes such as verifiability of the shares [9], [1], resistance of the scheme in the presence of a number of cheaters [10], [11] and dynamic change of the threshold and/or the number of participants [12], [13]. However, these schemes only work with a single secret and once the secret is changed to a new one, the system has to update the shares and resend the new shares to the participants. This consumes additional resources and might make the system impractical. Generalization of secret sharing scheme is a multi-secret sharing scheme where more than one secret to be shared [14] However, each participant receives one share at the beginning of the secret sharing process, the size of which is the same the size of the secrets. These schemes only provide computational security [15]. In 1994,

He and Dawson [16] proposed a multi-stage (t; n) threshold secret sharing scheme.

In 2007, Geng et al. [17] showed that the He-Dawson scheme is actually of one-time1545- Use and vulnerable to collusion attacks. They proposed a multi-use threshold secret sharing scheme using a one-way hash function. The term”multi-use” means that it is not required to redistribute the fresh shares over a secret channel to the participants, when a new set of secrets is to be shared. In 2006, Pang et al. [18] proposed a multi-secret

All the secret can work simultaneously and they can be recovered at single stage. The general access for sharing scheme structure in which all the key secrets revealed at same time i.e.) only authorized subset must participate their shares together. A multi-secret sharing scheme will be called multi-stage if in recovering a number of secrets, the reconstructed secrets do not leak any information about the unrecovered secrets. For this purpose,

Two securities must provide the combined with pseudo-secret shares depending on the original shares. All existing MSSS schemes are based on one-way (hash) functions [19], [20], [15], two-variable one-way Functions [21], [22] and assumptions such as hardness of solving discrete logarithm problem [23] which can now be tackled by quantum computers.

Advances in quantum computers threaten the security of currently used public-key Cryptographic algorithms, which is based on the difficulty of integer factorization and discrete logarithm problems. The introduction of quantum algorithms for factoring and computation of discrete logarithms by Shor in 1994 [24], has changed the research Trends from classical to post-quantum cryptography. In fact, the first post-quantum

Cryptographic system is the public key encryption scheme proposed by McEliece in 1978. It is based on hardness of coding problems, which is the beginning of code based Cryptography [25]. Not even quantum attacks have yet been known to represent a serious threat on the McEliece cryptosystem. From the efficiency point of view, no practical application of code-based cryptography is known because of the large size o the public key (100 kilobytes to several megabytes) [26].

Lattice based cryptographic constructions play a great role for post-quantum cryptography, because of its efficient linear computations. Furthermore, they enjoy provable security based on worst-case hardness of lattice problems. In addition, since no quantum algorithm has yet been proposed for solving lattice problems, lattice based cryptography is supposed to be resistant to quantum computers [26].

The first lattice based cryptographic algorithm was introduced by Ajtai in 1996 [27].

He proposed a construction of a family of one-way functions whose security is equivalent to the worst-case hardness of nc-approximate of lattice problems, where n is the Dimension of the lattice space and c is a positive constant. Goldreich et al. [28] proved that the Ajtai's function is collision resistant which is much stronger property than onewayness.

Some lattice based public key encryption schemes like GGH [29] and NTRU [30] have been introduced in literature and enjoy provable security based on hardness of lattice problems in worst case.

The cryptography is a very recent topic of an SSS design using lattice based (n:n)secret sharing scheme In2011 was proposed by Georgescu[31]whose security can be reduced. to the hardness of the secret scheme. This scheme offers the possibility for the participants to check if all the shares distributed by the dealer are valid. In 2012, Bansarkhani et al. [32] proposed an (n; n) threshold verifiable secret.

As well as the recovered secret to verify each participant to enable hash function based on linear lattice usage of sharing schemes. The security of this scheme relies on the hardness of nc-approximate shortest vector problem(SVP). This scheme uses efficient matrix vector operations to verify the shares instead of exponentiation used in conventional schemes. To the best of our knowledge, Aminiet al. [33] and Asaad et al. [34] proposed the first (t; n) threshold secret sharing schemeswith asymptotic security, in 2014. To recover the secret, the participants use Babai'snearest plane algorithm [35] to solve the closest vector problem (CVP) in general lattices.

Bendlin etc.And other sharing lattice trapdoor[37]using shamir's threshold secret sharing scheme of all have proposed two lattice based threshold decryption[36].

In this paper, we propose an MSSS scheme, in which the participants are each given one share to recover the secrets, in such a way that an adversary cannot recover theUnreconstructed secrets in polynomial time using the revealed secrets. In the proposed Scheme, lattice based one-way functions are applied to the original shares to obtain the corresponding pseudo-secret shares. Then, they are sent to the combiner for recovering the desired secret(s). The original shares and disclose the unrecovered secrets hence the combiner cannot misuse the pseudo secret shares will be obtained. The security of the proposed scheme is based on the hardness of lattice problems which are resistant to the quantum algorithms. Furthermore, the scheme enjoys significant features such as being multi-stage, multi-use and verifiable, and hence is favorable in many applications. Moreover, the scheme inherits its efficiency from simple matrix operations used in the secret sharing protocol, especially in the participants' side, and hence is suitable even
if the participants have limited processing capabilities.
The paper is organized as follows: Section 2 provides a brief review of lattices, lattice based cryptography and secret sharing schemes. Section 3 is dedicated to the proposed verifiable MSSS scheme including the security requirements and the algorithm. The security and efficiency of the proposed scheme are respectively discussed in Section 4 and Section 5. Section 6 concludes the paper.

2. EXISTING SYSTEM

- In cloud storage bloggers can let their friends view a subset of their private pictures or data; an enterprise may grant her employees access to a portion of sensitive data.
- The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage.
- Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and secure way to share *partial* data in cloud storage is not trivial.
- Increases the costs of storing and transmitting cipher texts.
- Secret keys are usually stored in the tamper-proof memory, which is relatively expensive.
- The costs and complexities involved generally increase with the number of the decryption keys to be shared.

3. OUR WORK

- An enterprise may grant her employees access to a portion of sensitive data can let their friends view a subset of their private pictures or data in cloud storage bloggers.
- The encrypted data from the storage of decrypt and send to other for sharing data, but it loses the value of cloud storage users can download the encrypted data and how effectively shares some challenging problems.
- As rights of the sharing data to others so that they can access these data from the server directly. Secure way to share partial data to finding an efficient in cloud storage is not trivial.
- Increases the costs of storing and transmitting cipher texts.
- Which is relatively expansive are in temper-proof memory, they are usually stored some secret keys. The costs and complexities involved generally increase with the number of the decryption keys to be shared.
- It can be fetched on demand from large but(non-confidential)cloud storage only a small part of number of cipher text classes has linear in to the public system parameters. The delegation of decryption can be efficiently implemented with the aggregate key, which is only of fixed size.
- Number of cipher text classes is large.
- It is easy to key management.

MICROSOFT VISUAL STUDIO 2008

Microsoft has a wide variety of products; we designed in ASP.Net and code Written in VB.net for front end designed. And as reports in Crystal Reports is built in Micro Soft Visual Studio 2008. Vb.Net is very flexible and easy to understand any application developer.

MYSQL

Fundamental part of the architecture in SQL server based on client/server relational database is a Microsoft SQL server (structural query language).

Structured Query Language (SQL)

To work with data in a database, you must use a set of commands and statements (language) defined by the DBMS software. There are several different languages that can be used with relational databases; the most common is SQL. Both the American National Standards Institute (ANSI) and the International Standards Organization (ISO) have defined standards for SQL. Most modern DBMS products support the Entry Level of SQL-92, the latest SQL standard (published in 1992).

SQL Server Features

Microsoft SQL Server supports a set of features that result in the following benefits:

Ease of installation, deployment, and use

SQL Server includes a set of administrative and development tools that improve your ability to install, deploy, manage, and use SQL Server across several sites.

Scalability

The same database engine can be used across platforms ranging from laptop computers running Microsoft Windows® 95/98 to large, multiprocessor servers running Microsoft Windows NT®, Enterprise Edition.

Data warehousing

SQL Server includes tools for extracting and analyzing summary data for online analytical processing (OLAP). SQL Server also includes tools for visually designing databases and analyzing data using English-based questions.

System integration with other server software

SQL Server integrates with e-mail, the Internet, and Windows.

Databases

A database in Microsoft SQL Server consists of a collection of tables that contain data, and other objects, such as views, indexes, stored procedures, and triggers, defined to support activities performed with the data. The data stored in a database is usually related to a particular subject or process, such as inventory information for a manufacturing warehouse.

SQL Server can support many databases, and each database can store either interrelated data or data unrelated to that in the other databases. For example, a server can have one database that stores personnel data and another that stores product-related data. Alternatively, one database can store current customer order data, and another; related database can store historical customer orders that are used for yearly reporting. Before you create a database, it is important to understand the parts of a database and how to design these parts to ensure that the database performs well after it is implemented.

DOTNET

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet/Intranet. The .NET Framework is designed to fulfill the following objectives:

- To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely.
- To provide a code-execution environment that minimizes software deployment and versioning conflicts.
- To provide a code-execution environment that guarantees safe execution of code, including code created by an unknown or semi-trusted third party.
- To provide a code-execution environment that eliminates the performance problems of scripted or interpreted environments.
- To make the developer experience consistent across widely varying types of applications, such as Windows-based applications and Web-based applications.
- To build all communication on industry standards to ensure that code based on the .NET Framework can integrate with any other code.
- . NET Support Remoting application.

The .NET Framework has two main components:

- The common language runtime.
- **.** NET Framework class library.

ADO.NET

ADO.NET provides consistent access to data sources such as Microsoft SQL Server, as well as data sources exposed via OLE DB and XML. Data-sharing consumer applications can use ADO.NET to connect to these data sources and retrieve, manipulate, and update data.

ADO.NET cleanly factors data access from data manipulation into discrete components that can be used separately or in tandem. ADO.NET includes .NET data providers for connecting to a database, executing commands, and retrieving results. Those results are either processed directly, or placed in an ADO.NET **Dataset** object in order to be exposed to the user in an ad-hoc manner, combined with data from multiple sources, or remoted between tiers. The ADO.NET **Dataset** object can also be used independently of a .NET data provider to manage data local to the application or sourced from XML.

ASP.NET

ASP.NET is a programming framework built on the common language runtime that can be used on a server to build powerful Web applications. ASP.NET offers several important advantages over previous Web development models:

Enhanced Performance**.** ASP.NET is compiled common language runtime code running on the server. Unlike its interpreted predecessors, ASP.NET can take advantage of early binding, just-in-time compilation, native optimization, and caching services right out of the box. This amounts to dramatically better performance before you ever write a line of code.

- **World-Class Tool Support.** The ASP.NET framework is complemented by a rich toolbox and designer in the Visual Studio integrated development environment. WYSIWYG editing, drag-and-drop server controls, and automatic deployment are just a few of the features this powerful tool provides.

- **Power and Flexibility.** Because ASP.NET is based on the common language runtime, the power and flexibility of that entire platform is available to Web application developers.

- **Simplicity.** ASP.NET makes it easy to perform common tasks, from simple form submission and client authentication to deployment and site configuration. For example, the ASP.NET page framework allows you to build user interfaces that cleanly separate application logic from presentation code and to handle events in a simple, Visual Basic - like forms processing model. Additionally, the common language runtime simplifies development, with managed code services such as automatic reference counting and garbage collection.

- **Manageability.** ASP.NET employs a text-based, hierarchical configuration system, which simplifies applying settings to your server environment and Web applications. An ASP.NET Framework application is deployed to a server simply by copying the necessary files to the server. No server restart is required, even to deploy or replace running compiled code.

- **Scalability and Availability.** ASP.NET has been designed with scalability in mind, with features specifically tailored to improve performance in clustered and multiprocessor environments. Further, processes are closely monitored and managed by the ASP.NET runtime, so that if one misbehaves (leaks, deadlocks), a new process can be created in its place, which helps keep your application constantly available to handle requests.

- **Customizability and Extensibility.** ASP.NET delivers a well-factored architecture that allows developers to "plug-in" their code at the appropriate level. In fact, it is possible to extend or replace any subcomponent of the ASP.NET runtime with your own custom-written component. Implementing custom authentication or state services has never been easier.

- **Security.** With built in Windows authentication and per-application configuration, you can be assured that your applications are secure.

a) Language Support
The Microsoft .NET Platform currently offers built-in support for three languages: C#, Visual Basic.Net, and JScript.

MODULES

- Secure Storage.
- Data Sharing
- Key Authentication.
- Integrity Checking.

SECURE STORAGE

- In this module, the user registration process is done by the admin...
- After registration every user will get an ID for accessing the cloud space.
- If any of the user wants to edit their information they have submit the details to the admin after that the admin will do the edit and update information process.
- In this module, every user's share their information and data's in their own cloud space provided by the admin.
- For providing security for their information every user's storing the information in their specific cloud.
- Registered users only can store the data in cloud.

DATA SHARING

- In this module, the encrypted data or information stored in the cloud is forwarded to another user account by using that user's public key.
- If any user wants to share their information with
Their friends or someone they can directly
Forward the encrypted data to them.

KEY AUTHENTICATION

- In this module, the information and data's shared by the user in the cloud is encrypted by using AES algorithm.
- All the information shared by every user is encrypted based on the data sensitivity and stored in the cloud.
- The two actions are access control and permission control.
- Access control process is based on the server control features.
- Permission control process is based on the client control features.

INTEGRITY CHECKING

- Integrity checking is the process of comparing the encrypted information with altered cipher text.
- If there is any change in detection a message will send to the user that the encryption process is not done properly.
- If there is no change in detection means then it will allow doing the next process.
- In this module, the encrypted data is decrypted by the user using the public key of owner of the data.
- AES algorithm is used for encrypting and decrypting the information. The user can view the data and also can download the data with high security.

CONCLUSIONS

In this paper, we have considered a generalization of a secret sharing scheme which we
call multi-stage secret sharing scheme. The desired level of security in such schemes is the computational security. In an MSSS scheme, the secrets may be recovered at different stages. The participants use pseudo-secret shares derived from their original shares to recover the secrets. In the proposed scheme, we obtain the pseudo-secret shares from the shares using lattice based one-way functions introduced by Ajtai. The new scheme is multi-stage, multi-use, verifiable, and provides the computational security based on the worst case hardness of lattice problems which makes it secure against quantum computers. Moreover, the scheme is significantly efficient in the participants' side and
is suitable even if the participants have limited processing capabilities

REFERENCE

[1] Eric Zavattoni, Luis J. Dominguez Perez, Shigeo Mitsunari, Ana H.S´anchez-Ram´ırez, Tadanori Teruya, and Francisco Rodr´ıguez-Henr´ıquez. Softwar implementation of an attribute-based encryption Scheme. IEEE Trans. Computers, 64(5):1429–1441, 2015.

[2] Erik C Shallman. Up in the air: Clarifying cloud storage protections.

a. Intell. Prop. L. Bull., 19:49, 2014.

[3] Cheng-Kang Chu, Sherman SM Chow, Wen-GueyTzeng, JianyingZhou, and Robert H Deng. Key-aggregate cryptosystem for Scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions on, 25(2):468–477, 2014.

[4] Secure sharing of personal health records in cloud computing attribute-based encryption and Ming Li shucheng Yu,Yao Zheng,Kui Ren,and Wenjing Lou scalable of parallel distributed systems in IEEE Transaction on 24(1):131-143,2013.

[5] In pairing –based cryptography

[6] International conference on pairing 2013 .Beijing china, November 22-24,2013,revised selected papers pages 229-250,2013 and arithmetic pairing of Chitchanok chuengsatian sup,Michael Naehrig,PanceRibarski and petor Schwa be Panda.