

A Novel Method for Effective Detached Group Key Managing Scheme Using Hierarchical Method of Cryptography

Chetna Panwar

*Computer Science Department
MIST, Indore (M.P), India*

Pankaj Dashore

*Computer Science Department
MIST, Indore (M.P), India*

Abstract: Data access control has becoming a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a trusted cloud storage system. Elliptic Curve Cryptography is regarded as one of the most suitable technologies for security in cloud storage. In almost all existing schemes, it is assumed that there is only one authority in the system responsible for issuing to the users. Secure and reliable group communication is an active area of research. The central research challenge is secure and efficient group key management. In this paper, we propose an efficient group key management protocol in distributed group communication. This protocol is based on Elliptic Curve Cryptography and decrease the key length while providing securities at the same level as that of other cryptosystems provides. It is our best try to address the single point bottleneck on both security and performance.

Index Terms: Elliptic curve Cryptography, management protocol, Cryptosystem, Distributed Network

I. INTRODUCTION

The cloud computing becomes the hot issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode in the industry. Entirely based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The users can access your applications and data from anywhere. When data has been distributed it is stored at more locations increasing the risk of unauthorized physical access to the data. For example, in cloud based architecture, data is replicated and moved frequently so the risk of unauthorized data recovery increases dramatically. (e.g. disposal of old equipment, reuse of drives, reallocation of storage space)[3]. the manner that data is replicated depends on the service level a customer chooses and on the service provided that encrypts data prior to uploading it to the cloud. The cloud computing changed the style of software. The data can be stored in the cloud system and the user can use the data in any time and in anywhere. The data often stored in the private or personal system such as PC. The cloud computing can guarantee the data security and the user do not protect the data by himself again. So the cloud computing must ensure the security of data stored in the cloud system. Many companies provide the cloud computing platform such as Google, IBM, Microsoft.

As the cloud computing system has more data which may be the private data of user, the data must not be destroyed or grabbed. Because the data in the cloud system may be important for the user, the hacker may pay more attention to get the data. The system must be protected more carefully than the traditional system. The company uses the cloud system and stores the data in it. The data can be seen by other people who are not person of company. The company must have confidence in the cloud computing if they want to store the private data in the cloud system. Governance and security are crucial to computing on the cloud service provider's infrastructure, if the cloud system is in firewall or not[4].

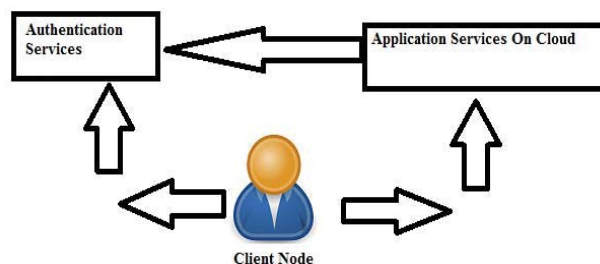


Fig-1: User Communication

The security of cloud computing is the key import problem in the development of cloud computing. The traditional security mechanism cannot protect the cloud system entirely. The cloud computing application is no boundaries and mobility and can lead many new security problems. The main security issues include data security, client data security assurance, cloud computing platform dependability and cloud computing organization. The cloud system is running in the web and the security issues in the web additionally can be found in the cloud system. The cloud system is not distinctive the customary system in the PC and it can meet other uncommon and new security issues. The greatest worries about cloud computing are security and protection. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is usually Internet-based computing. The cloud is a metaphor for the Internet based on how the internet is described in computer network diagrams; which means it is an abstraction hiding the complex infrastructure of the internet. It is a style of computing in which IT-related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet ("in the cloud") without knowledge of, or control over the technologies behind these servers[5].

II. LITERATURE SURVEY

The underlying concept dates back to 1960 when John McCarthy expressed his opinion that "computation may someday be organized as a public utility" and the term Cloud was already in commercial use in the early 1990s to refer to large ATM networks. By the turn of the 21st century, cloud computing solutions had started to appear on the market, though most of the focus at this time was on Software as a service. Amazon.com played a key role in the development of cloud computing when upgrading their data centres after the dot-com bubble and providing access to their systems by way of Amazon Web Services in 2002 on a utility computing basis. They found the new cloud architecture resulted in significant internal efficiency improvements.

In the paper [6], Group key management is a difficult task in implementing large and dynamic secure multicast. In this paper, a new scheme is proposed in the basis of in-depth analysis of the requirements of the secure multicast and group key management. The scheme is based on the multicast group security architecture and multicast security group key management architecture proposed by IETF. This scheme constructs group key based on pairings and distributes the group key using HSAH function polynomial, and manages group key making use of the dynamic layering GCKS. The scheme is better in security, lower in computation cost and communication cost. The analysis comparison proves that the scheme has strong scalability and efficiency.

In this paper [7], A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other, most frequently using a multi-hop wireless network. Nodes do not necessarily know each other and come together to form an ad hoc group for some specific purpose. Key distribution systems usually require a trusted third party that acts as a mediator between nodes of the network. Ad hoc networks typically do not have an online trusted authority but there may be an off line one that is used during system initialization. Group key establishment means that multiple parties want to create a common secret to be used to exchange information securely. Without relying on a central trusted entity, two people who do not previously share a common secret can create one based on the party Diffie Hellman(DH) protocol.

This idea [8,9] security of sensor networks has become one of the most pressing issues in further development of these networks. Compared to the traditional wireless network, Wireless Sensor Network (WSN) provides a different computation and communication infrastructure. These differences originate

not only from their physical characteristics, but also from their typical applications. For example, the physical characteristics include the large scale of deployment, limited computing capability, and constraints on power consumption.

In this paper [10,11] the requirements for the key management of a WSN are noticeably different from those for traditional networks. The major requirements for the key management in a WSN are as follows. First, sensor's communication involves a key distribution procedure between the communication parties, in which the key may be transmitted through some insecure channels.

III. PROBLEM STATEMENT & PROPOSED SOLUTION

In existing system, Cryptographic techniques were applied to access control for remote storage systems. The data owners encrypt files by using the symmetric encryption approach with content keys and then use every user's public key to encrypt the content keys. It requires each data owner to be online all the time. Some methods deliver the key management and distribution from the data owners to the remote server under the assumption that the server is trusted or semi-trusted.

Drawbacks of the existing system:

- The key management is very complicated when there are a large number of data owners and users in the system.
- The key distribution is not convenient in the situation of user dynamically system.
- The server is cannot be trusted by the data owners in cloud storage systems.
- It cannot be applied to access control for cloud storage systems.

To overcome the above problem we propose an efficient group key management protocol in distributed group communication. This protocol is based on Elliptic Curve Cryptography and decreases the key length while providing securities at the same level as that of other cryptosystems provides. We provide the high level security and avoid the replication of file in the cloud service provider. In proposed system, we are using hash function to generate key for the file .By using hash function to avoid the duplication in cloud. After that we are applying cryptographic technique for security purpose. We using ECC algorithm for encryption and decryption process.

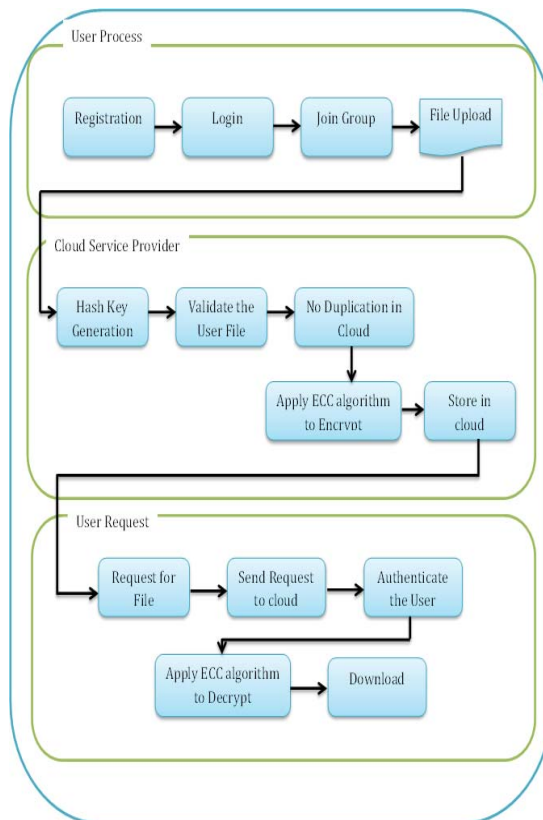


Fig-2: Proposed Architecture

Utility of the system:

- Avoid duplication in cloud.
- Increase the security level.
- High efficient.
- ECC algorithm provides high end security.

Proposed Steps of Algorithm:

- Firstly users register their self by filling the registration details. Then login by their username and password.
- After that user join the group and the key will generated.
- The generated key will help for knowing the user is authenticated or not.
- Then users upload the file. Then hash key is generated for validate the user file.
- After that applying an ECC algorithm for encryption.
- Subsequently, user request to the cloud for file then ECC algorithm is applied for decryption.
- We can download the file at our destination.

IV. RESULT EVALUATION

In to implement them equipment and programming assets are required, henceforth the rundown of fancied assets and their specialized details are given in this section. Moreover of that, this segment incorporates the re-enactment parameters and executed system situations. This segment of the archive gives comprehension of recreation and its determinations in subtle element. Beforehand talked about part examination and outline of wanted framework is finished, yet.

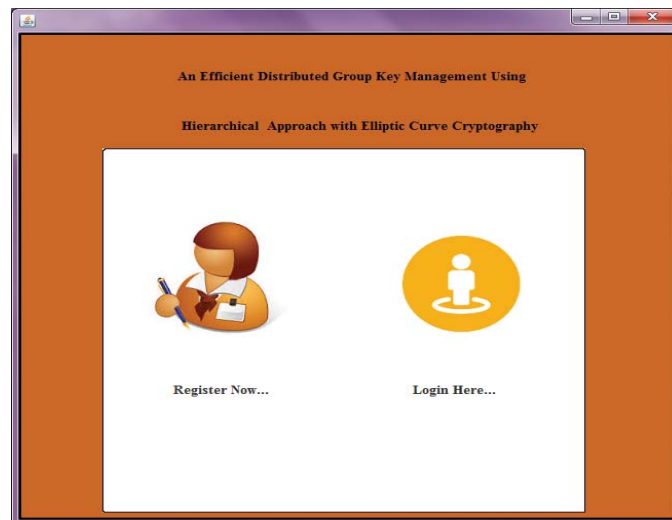
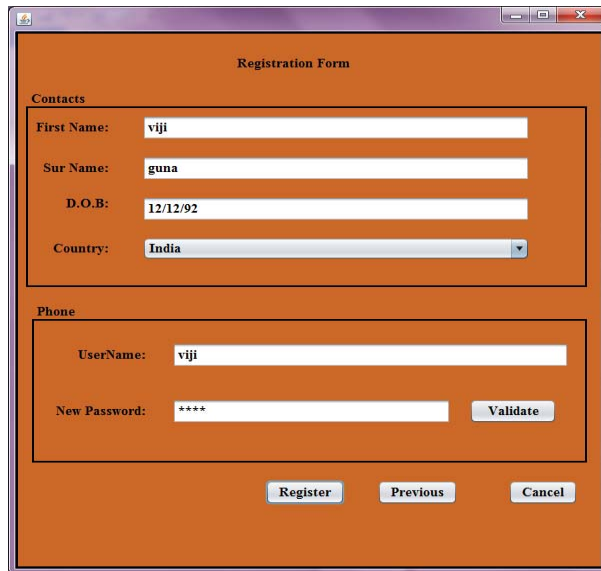
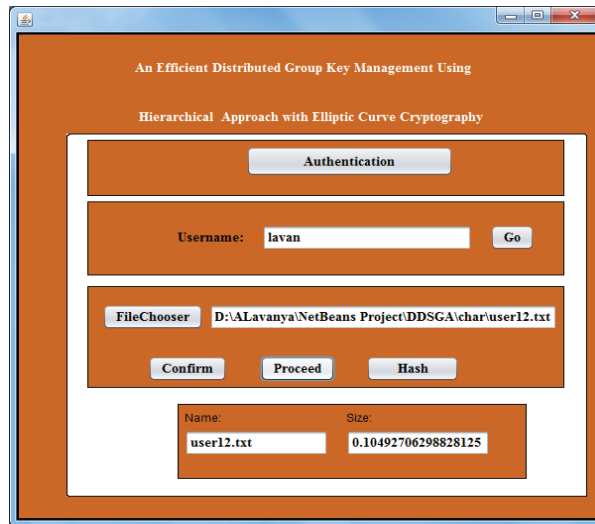


Fig-3: Login Window



The image shows a 'Registration Form' window with a brown background. It is divided into two main sections: 'Contacts' and 'Phone'.
In the 'Contacts' section, there are four input fields: 'First Name' with the value 'viji', 'Sur Name' with the value 'guna', 'D.O.B' with the value '12/12/92', and 'Country' with a dropdown menu set to 'India'.
In the 'Phone' section, there are two input fields: 'UserName' with the value 'viji' and 'New Password' with the value '****'. A 'Validate' button is located to the right of the 'New Password' field.
At the bottom of the window, there are three buttons: 'Register', 'Previous', and 'Cancel'.

Fig-4:Registration form window



The image shows a 'Key generation window' with a blue border and a brown background. The title is 'An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography'.
The window contains several components:
1. An 'Authentication' button.
2. A 'Username' field with the value 'lavan' and a 'Go' button.
3. A 'FileChooser' button and a text field containing the path 'D:\ALavanya\NetBeans Project\DDSGA\char\user12.txt'.
4. Three buttons: 'Confirm', 'Proceed', and 'Hash'.
5. A table at the bottom with two columns: 'Name' and 'Size'. The 'Name' column contains 'user12.txt' and the 'Size' column contains '0.10492706298828125'.

Fig-5:Key generation window

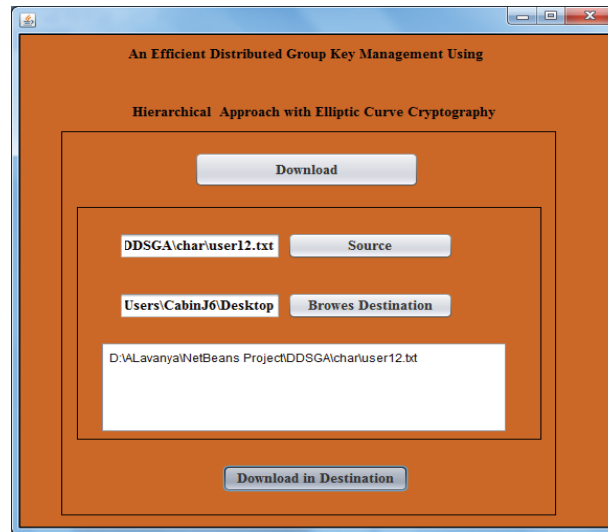


Fig-6:File upload and download window

V. CONCLUSION

For asymmetric key, Elliptic Curve Cryptography key agreement is introduced. We have used Elliptic Curve Cryptography and it provides much stronger security with smaller key size. It Validate the confidential File in cloud and efficiently work. We using ECC algorithm for encryption and decryption process to decrease probability of attacking the file. Key administration is a crucial cryptographic primitive upon which other security primitives are constructed. On the other hand, there are numerous current key administration plots that need on some focuses and those are very little suitable for specially appointed systems. In this paper we are going to introduce a circulated various levelled bunch key administration approach that uses Elliptic Curve Cryptography for secure era and appropriation of gathering key.

REFERENCES

- [1] Fan, Ping, Kuan and Ming, "A Dynamic Layering Scheme of Multicast Key Management," 5th IEEE International Conference on Information Assurance and Security, Xian, China, Vol. 1, pp. 269-272, August 18-20, 2014.
- [2] Suresh Kumar B. and Jagathy Raj V. P. "A Secure Encryption mechanism based on secure system on IBE, DNS and Proxy Service" Journal of Emerging Trends in Computing and Information Sciences©2009-2012 CIS Journal.
- [3] Muhammad Yasir Malik Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor, ICACT 2010, ISBN 978-89-5519-146-2 Feb. 7-10, 2010.
- [4] Ye, Zhao, and Guo, "A Safety Group Key Management Scheme in Mobile Adhoc Network," 8th IEEE International Conference on Reliability, Maintainability and Safety, Chengdu, China, pp. 512-515, July 20-24, 2009.
- [5] Chen, Lin, Shen, Hashimoto and Kato, "A Group-Based Key Management Protocol for Mobile Ad Hoc Networks," IEEE Global Telecommunications Conference, Honolulu, Hawaii, pp. 1-5, November 30- December 04, 2009.
- [6] Shoufan and Huss, "High-Performance Rekeying Processor Architecture for Group Key Management," IEEE Transactions on Computers, Vol. 58, Issue 10, pp. 1421-1434, October 2009.
- [7] Dawood, Mneney, Aghdasi and Dawoud, "An Efficient Hierarchical Group Key Management Protocol for Mobile Ad-Hoc Networks," IEEE 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Aalborg, Denmark, pp. 619-623, May 17-20, 2009.
- [8] McGrew and Sherman, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," IEEE Transactions on Software Engineering, Vol. 29, Issue 5, pp. 444-458, May 2003.
- [9] Lauter Kristin, "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 62-67, February 2004.