Providing Data Protection as a Service in Cloud Computing

Sunumol Cherian[*], Kavitha Murukezhan[**]

[*] Department of computer Science, Vedavyasa Institute of Technology, Calicut
[**] Head of computer science Department, Vedavyasa Institute of Technology

Abstract- Data protection in cloud has become an unavoidable and tremendously increasing technology. Many multinational organizations are interested in cloud computing and its wonderful features but they are worried about the security, privacy and availability of data as it rest in the cloud. As more and more sensitive information are centralized in cloud the data protection, security and privacy issues must be tightly considered. In this paper we propose a new cloud computing service called *Data Protection as a Service*. User authentication, data protection, security are the key areas we consider. User authentication is provided using alphanumeric password and graphical password, security is provided using encryption of the file using key. Key management is an important concept used for the protection of data. Overall transactions are viewed by an auditor. Here multilevel data protection is guaranteed for the cloud users.

Index Terms- Cloud data protection, graphical password, key, encryption, and auditor.

I. INTRODUCTION

As cloud computing has become important and easy to implement, many multinational organizations and leading companies are coming forward for adopting the cloud features for the better management and increasing efficiency of their organization. Cloud computing provides on-demand high quality data storage service. But there is one factor that everybody is afraid about cloud computing is the security problems. Since all the data are stored in the cloud environment data owners are afraid about the security. Whether hackers will attack the data? This question makes a good scene. For that sensitive data usually should be encrypted prior to outsourcing for data privacy and avoiding unauthorized accesses. However, data encryption makes effective data utilization a very risky task given that there could be a huge volume of outsourced data files.

In Cloud Computing, data owners share their outsourced data with a large number of cloud users. Each user might be interested in retrieving only a specific data file in a given session. Also it must be *guaranteed* that only authorized users must have the permission to view the data file. User authentication can be performed by using many scientific ways. Alphanumeric passwords and graphical passwords are both guaranteed service. In many of the trusted website like Gmail, Google all supports alphanumeric passwords. They also provide multiple protection techniques like verification using mobile number, captcha etc. Multilevel verification ensures the authorized access. The concept of key come from the branch of science called cryptography. There are basically two types of keys they are public key and private key. A public key is known to everyone and a private or secret key known only to the recipient of the message. An authorized user has the key for encryption and decryption of the specific data file. Keyword based search is one of the popular ways to selectively identify and retrieve data files instead of retrieving all the files. Keywords are parts of file name or phrases used in the file which will help us to find the exact data file at the time of retrieval if you don't remember the exact keyword. There are many keyword searching methods.

An auditor is one who keeps track of all the histories of users. In our paper we use software that will keep the histories of all the users and all the data file transactions etc... Thus data protection is highly verified in our system, so the cloud users can outsource the data very securely.

II. RELATED WORK

2.1 Fuzzy Keyword Search over Encrypted Data in Cloud Computing. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing. This technique formalizes and solves the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads**.**

2.2 Cloud Data Protection for Masses. This paper proposes a new cloud computing paradigm, data protection as a service. DPaaS is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications. Data protection is provided by using three primitives they are access control, key management and logging. Also there is an auditor who audits all the transactions occurred in the system. Auditor finally provides an audit report based on all conversations.

2.3Graphical User Authentication: A Time Interval Based Approach. A number of authentication techniques have been proposed in the recent times that are based upon graphical methods. Text based passwords are most commonly used for

authentication; however, they are highly vulnerable to several kinds of attacks. Graphical techniques are coming up as an attractive alternative to the conventional methods of authentication. In this paper we have proposed a graphical method of authentication that employs graphical coordinates along with a novel introduction of time interval between successive clicks. The user needs to recall the coordinates and the time interval of the successive clicks. This leads to the incorporation of the advantages of the recent graphical methods along with the added security achieved through the use of time interval. The proposed scheme has a much higher password space than the other contemporary graphical authentication schemes. The scheme is robust, secure and very convenient to use.

III. RESERCH ELABORATIONS

Security of data

For the security in storage most system uses data protection mechanisms. They include graphical password, alphanumeric password and many other similar ways that will help us to increase the security of data.

Authorization

Only authorized user has the permission to read and edit the file that is stored in the cloud. Authorized users are those users who have cloud authorization and also should have the right to retrieve the data file. All the users who have the cloud access are not allowed to access the data file, but all users who can access a particular data file stored in the cloud are cloud authorized users.

Reliability

Reliability is also as important as security. Reliability in storage corresponds to the accuracy and consistency of data.

There are different cloud storage systems. Some are focused on storing e-mail messages or digital pictures etc. In this paper we propose a system which is able to be secure storage of files by using alphanumeric passwords, graphical passwords, key management and auditing. Thus in our proposed system we provide data security as a service for the data stored in the cloud by undergoing various strategies.

IV. THEORIES AND APPROACHES

4.1. Alphanumeric Password Authentication

In our system there is an administrator who has the overall control . Both the administrator and staffs have alphanumeric password authentication. Only the users who passed the text can only enter into the next level of authentication. This administrator has the rights to create the users. Administrator has cloud authorization. Users created by the administrator have only the cloud access.

4.2. Graphical Password Authentication

Both the administrator and the users should undergo the graphical password text. In view of the shortcomings of the traditional approach to authentication, i.e. alphanumeric passwords, Graphical techniques are gaining importance. A graphical password is an authentication system in which the user has to work with images, either selecting them or creating them. The graphical password form is shown in Figure 4.2. E.g. the user may select some points from the image which is stored as the graphical password in the database. If someone needs to store the file or retrieve the file stored in the system he should enter the correct graphical password for access to the file. The graphical-password approach is also sometimes called graphical user authentication (GUA). A graphical password is easier to remember than a complex text-based password for most people.

Figure 4.2: Graphical Password

4.2. Key Management

The concept of key come from the branch of science called cryptography. There are basically two types of keys.

1. Public key
2. Private key

A public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it. In our system we encrypt the file using a key and stored in the cloud. The user should enter the key to decrypt the file. The key management form is shown in Figure 4.3.So multiple protection mechanisms are used here for protecting the files in the cloud.

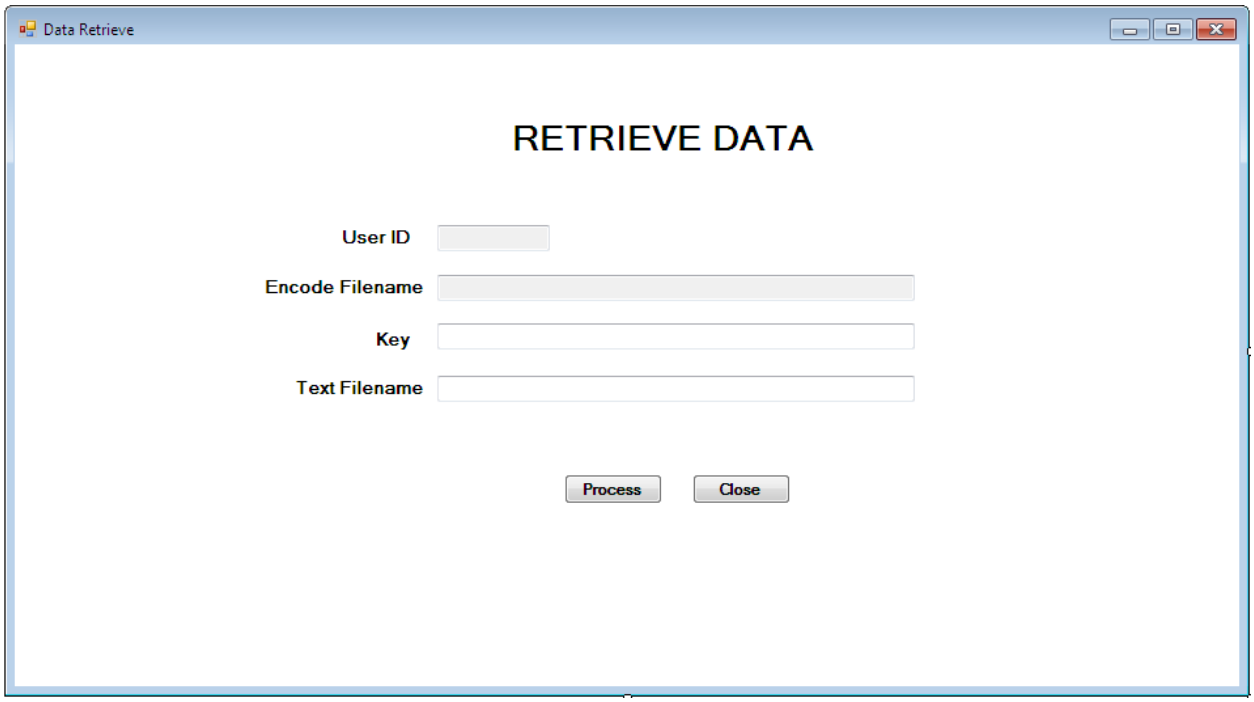

Figure 4.4: Key Management

4.3. Auditor

The auditor is one who audits the overall performance of the system. He can track the transactions and logins of users with correct time and date. Here auditor is software that is capable of tracking the transactions. Cloud storage offers movement of data into cloud .It has great convenience to the user because users can store their data in the cloud safely without the knowledge about the storage space . There are several trends in cloud computing because of its wide variety of possibilities in the new era. Security in cloud computing have greater importance because users wants their data to be secure .The attacks towards the data which is stored into the cloud is increasing. There are different security services implemented toward data storage. Researches for the security threats in cloud have great opportunities.

All the existing systems have many drawbacks and also they do not fulfill the motive. So here we introduce a new data protection mechanism which incorporates many technical concepts of computer science engineering. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography include s the concepts of keys, public key and private key, so we are familiar with the concept of keys. An authorized user must know the key used for locking and unlocking the data. Here in our system the administrator has the ultimate power. He creates the users in the cloud. Each user must login using 2 ways. The workflow of the model is shown in Figure 4.4.1 and in Figure 4.4.2.Once is by using character password after passing that he should login using graphical password.

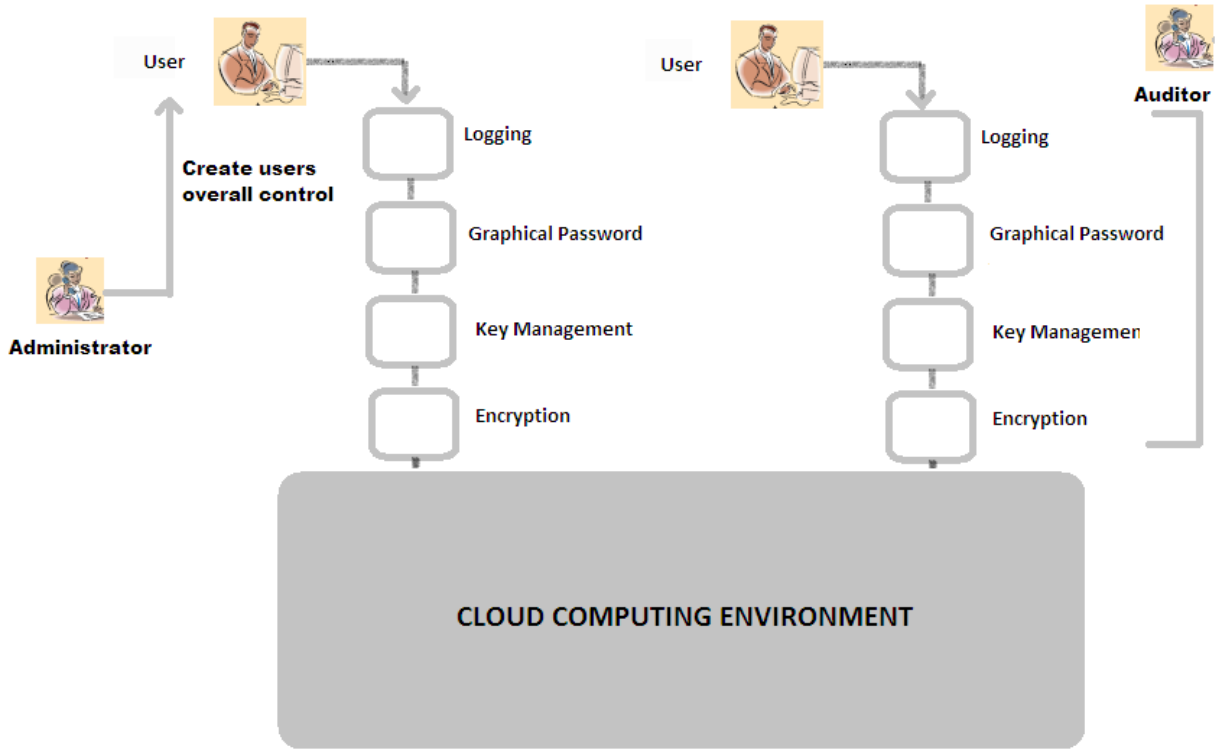

Figure 4.4.1: Workflow of the model

After they login they can communicate each other and sent files between them. The receiver must know about the key used by the sender otherwise he cannot decrypt the file. There is an auditor who is tracking all the transactions and all the conversations between the users. The auditor is basically software that can track all the transactions. So multilevel data security is provided in our model.

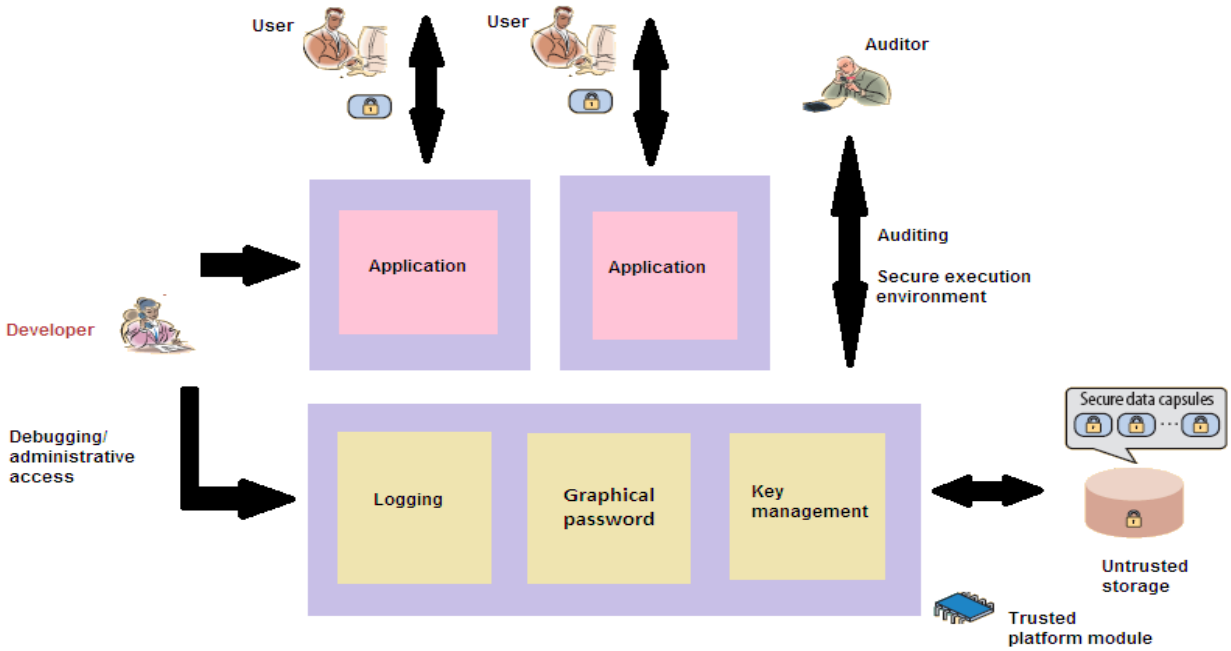

Figure 4.4.2: Data Protection as a service in Cloud Computing

V. CONCLUSION AND FUTUREWORK

As private data moves online, the need to secure it properly becomes increasingly urgent. The good news is that the same forces concentrating data in enormous datacenters will also aid in using collective security expertise more effectively. Adding protections to a single cloud platform can immediately benefit hundreds of million users

In future, this work can be extended to develop a more formal model for data protection as a service in cloud computing. We can use this model for many other communications like client server communication etc..

REFERENCES

[1] C. Dwork, (2007) "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, pp. 496-502.

[2] C. Gentry, (2009) "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory Computing(STOC 09), ACM, pp. 169-178.

[3] E.Naone,(2011) "The Slow-Motion Internet," Technology Rev., Mar./Apr. www.technologyreview.com/files/54902/GoogleSpeed_charts.pdf.

[4] A.Greenberg, (2011) "IBM's Blindfolded Calculator," www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html.

[5] P.Maniatis et al.(2011), "Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection,"Proc. 13th Usenix Conf. Hot Topics in Operating Systems (HotOS 11), Usenix,; www.usenix.org/events/hotos11/tech/final_files/ManiatisAkhawe.pdf.

[6] S. McCamant and M.D.(2011) Ernst, "Quantitative Information Flow as Network Flow Capacity," Proc. 2011 ACM SIGPLANConf. Programming Language Design and Implementation (PLDI 08), ACM, pp. 193-205.

[7] Birget, J.C., Hong, D., and Memon, N.Robust discretization, with an application tographical passwords. Cryptology ePrint Archive.http://eprint.iacr.org/168 accessed January17.

[8] Blonder, G.E. (2011). Graphical Passwords.United States Patent 5559961.Boroditsky, M. Passlogix password schemes.http://www.passlogix.com.

[9] Brostoff, S. and Sasse, M.A. (2011). ArePassfaces more usable than passwords: A f ieldtrial investigation. In McDonald S., et al. (Eds.),People and Computers XIV - Usability or Else,Proceedings of HCI 2000, Springer, pp. 405-424.

AUTHORS

First Author – Sunumol Cherian, Department of computer Science, Vedavyasa Institute of Technology, Calicut, Email: sunuharsh@gmail.com, Phone: 9961240454
Second Author – Kavitha Murukezhan, Head of computer science Department, Vedavyasa Institute of Technology, Email: hodcse@vedavyasa.org, Phone:9447900607