International Journal of Grid Distribution Computing
Vol. 8, No.5, (2015), pp.153-164
http://dx.doi.org/10.14257/ijgdc.2015.8.5.15

Securing Mobile Cloud Environment with Unified Reliable Encryption Algorithm, Security Key and Authentication

Buchanagandi Enock Nyamajeje[1] and Huiqun Yu[1,2]

Department of Computer Science and Engineering
[1]East China University of Science and Technology, 200237, China
[2]Shanghai Key Laboratory of Computer Software Evaluating and Testing, Shanghai 201112, China
yhq@ecust.edu.cn, buchana92@yahoo.com

Abstract

Building applications on on-demand infrastructures instead of building applications on fixed and rigid infrastructures was provided by cloud computing providers. By simply positing into the cloud, it gains fast access to business applications or infrastructure resources with reduced Capital Expenditures (CAPEX). Dramatic increase in amount of information's are placed into the cloud by individuals and industries, security issues are vital concern in mobile computing (MCC) and impends fast deployment of applications on the cloud. This work discus the different security issues that arises about how safe the mobile cloud computing environment is and provides a unified reliable security mechanism. There are two different types of the cloud users are: On-demand and Optimistic. On-demand is a non-preemptible for flexible leases given a user accessing to the resources within an interactive time of making the request and makes the resources available for an agreed-upon period of time, user can deploy any virtual machine (VM) compatible with the system. Optimistic is preemptible and pre-set contract gives a user access to resources at an indeterminate time and make resources available to the user for an insufficient amount of time. After that, this resources are initially (pre)-defined for the user by the cloud admin, that is the user cannot provide his or her own virtual machine (VM) based on defined access control for security.

Keywords*: On-demand user, optimistic user, security, cloud, mobile environment*

1. Introduction

As more and more data files are being outsourced into the cloud, end users and providers of mobile devices enjoy the on-demand access to the cloud storage services. In this project we discuss the different security issues that arise about how safe the mobile cloud computing environment and outsourced data files is at risk. The list of examples for cloud computing security are identified and discussed which needs to be understood and assess the risks associated. Mobile Cloud Computing (MCC) is exploring vastly change in IT due to anywhere anytime data access. Mobile devices are enabled with rich user experience especially, Smart phones. Apple, Google, facebook and Amazon are the top four horsemen in the mobile world. Then mobile cloud computing technology is growing rapidly among the users and at the same time it introduces the new security malice. A lot of questionnaires are being carried out to eradicate the issues to make IT more reliable and secure because more precious data is stored in the cloud space [1], [2]. As the Internet-enabled mobile devices including smart phones and tablets continue to grow, web-based threats will continue to increase in large number to make more difficult to provide security services to the outsourced data.

Securing data is more crucial in the Mobile Cloud Application Environment [3], [4]. In the existing system, the growth of Internet online services has been very quick of the

ISSN: 2005-4262 IJGDC

last decades [17]. Each online service requires Internet users to create a new storage space to use the service. The drawback can be seen when every user actually needs more than one service and, consequently, has numerous accounts. The users are depending upon the cloud storage. These numerous accounts have to be managed in a secure and, simple way to be protected against suspicious identity theft internal and, external of the storage services. All services are using the cloud and storage environment .The security level is also less compare; services are common for all the end users. So users are not interest in mobile cloud environment. Dis-advantages being: (1) User compatibility is less (2) security based services are not available.

After analyzing the existing solution and their problems as mentioned in the above paragraph, the thesis present a unified secure mobile cloud environment framework that deploys a hybrid Cloud model and its support for security service provisioning, to secure the exchange of data between an application running on the mobile devices and in cloud. Considering to resource constraint limitation on mobile devices, we propose security level access control that don't enforce security measures to data transmitted between the running application components in cloud and those data exchange between mobile and cloud, which meet security requirements for the end-user. Moreover, allows the end user to choose security level depending on their demands and apply to their data up on their different requirements and preferences such as energy, storage and cost for using cloud resources and space. This project aim is to identify, classify a common and possible attacks on data transmitted between mobile device components and component-based mobile cloud application, by applying information security mechanisms, infrastructure security, security countermeasures within and from all applications in mobile cloud space, while trying to unify the security functions used in different layers, mostly considering basic conceptual layers in the network layer, transport layer, and the user application layer which are subjected to security threats. This work discusses the different security issues that arise about how safe the mobile cloud computing environment is. There is different type of cloud users (1) On-demand user is a non-pre-emptible for flexible leases given a user access to a resource within interactive time of making the request and makes the resource available for an agreed-upon period of time. The user can deploy any VM compatible with the systems and (2) other user type is Optimistic user, optimistic user is a re-emptible and pre-set contract that give a user access to a resource at an indeterminate time and make the resource available to the user for an insufficient amount of time. After that, this resource is initially (pre)-defined for the user by the cloud admin, that is the user cannot provide his or her own virtual machine (VM).

The rest of this paper is organized as follows: Section 2 describes the system design; Section 3 outlines the main related work; Section 4 presents the proposed protocol explaining the steps of the design system roles; Section 5 present a simple analyzes of the scenario which describes the functionality and applicability of the system design; Section 6 summarizes with main conclusion and future work.

2. Methods and System Design

A. Security System Model

Proposed network architecture for mobile cloud applications/services in cloud mobile environment is illustrated in Figure 1. In this security system model we outline four different conceptual network entities can be identified as follows:

- User: end user of mobile devices access to cloud storage, has data to be stored and for data to be transmitted between mobile and cloud for both individual consumers and industries.

- IIAS Cloud Framework: Intelligent Insurance Analytics Systems cloud framework -It consists of a policy storage module which stores and manages access control policies and act as a Policy Administrative Management Domain (ADMD) level.
- Security Based: is a security choice broke on security level access control based on cloud services for all User-types i.e. On-demand user and Optimistic user.
- Cloud admin: manages user and the system can access services for the defined access control for security and issues access key. On addition, cloud admin does the only role/security assignment (i.e., responsible to know access control for security) such as admin access on-demand user Cloud storage; security level one file access, security level two file access; and view all user details (i.e., public auditing).

In mobile cloud environment, users are storing and retrieving the file through IIAS Cloud Framework into cloud server between the application components running in mobile device and those running in cloud. The architecture has to be able to adapt forms of choice from anyone according to type of cloud user security based choice of the services. Users interact with cloud server via cloud service provider to access or retrieve their data, user have an option on a choice for type of users (i.e. On-demand users or Optimistic users) based on our system model. Before, choice for type of users, user is authenticated and reliable, equipped with security means (such as RSA Diffie-Hellman algorithm) to encrypt data to assure users that their data are being correctly stored and maintained.

In our model, to guarantee the confidentiality of data stored in the cloud. Database encryption is provided at the file or column level. The steps in encrypting a database are: Determine the criticality of the need for encryption, determine which algorithms best suit the encryption standard. These algorithms generate keys related to the encrypted data. Encrypted data are contained in encrypted tables stored in cloud generates the corresponding encrypted table and a unique encryption key. The name of the encrypted table is computed by encrypting the name of the plaintext table through that key. The encryption algorithm used for encrypting the table names is a standard AES algorithm in a deterministic mode corresponding encryption key are able to compute the name of the encrypted table. The deterministic scheme is preferred because it allows a correspondence between plaintext, and encrypted tables, improves the efficiency of the query translation process. On the other hand, user may perform file blocks operations on his data, file upload, send to cloud, packet sending, and download are forms of operation we are considering. Figure 1 shows the architecture of the mobile cloud security model.

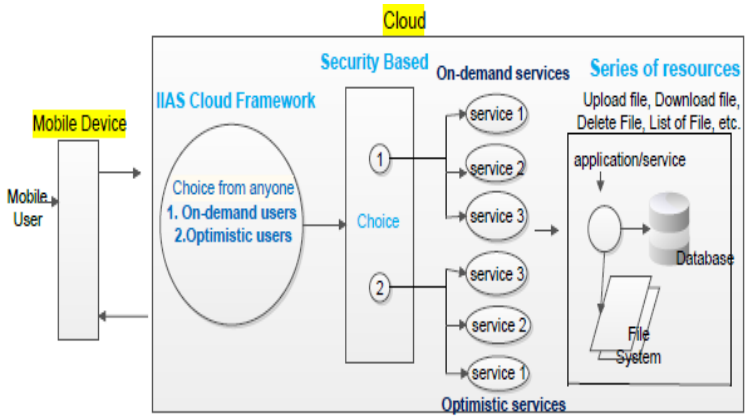


Figure 1. Mobile Cloud Security Model

Optimistic users: In this type of users are also using the cloud environment in rental basics. These users are using the cloud environment in short period with low cost. Here also some services are provided, but security is less than the on- demand users.

On demand Users: On demand users are taking and using the cloud environment in a rental base. On demand users are using the cloud environment in lease agreement. In this type of cloud users are using the cloud environment in more security manner compared to optimistic users. These users are storing and retrieving the file in more security manner, there we are providing the more securities and access control for the access that file.

B. Cloud Storage Module

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

C. Mail Authentication

Email authentication is a collection of techniques aimed at equipping messages of the email transport system with verifiable information. It is a coarse-grained authentication, usually at Administrative Management Domain (ADMD) level, and implies no sort of authorization. That is, the purpose of email authentication is to validate the identities of the parties who participated in transferring a message, as they can modify the message. The results of such validation can then be used in delivery decisions, which are beyond the scope of email authentication proper, and are quite different in nature from.

D. File Stored Block Model

We show that even some stored file blocks have been lost; the server is able to generate a valid proof by replacing a pair of lost data block and its signature with another block and signature pair. We also provide a solution to the problem while preserving all the desirable features of the original protocol.

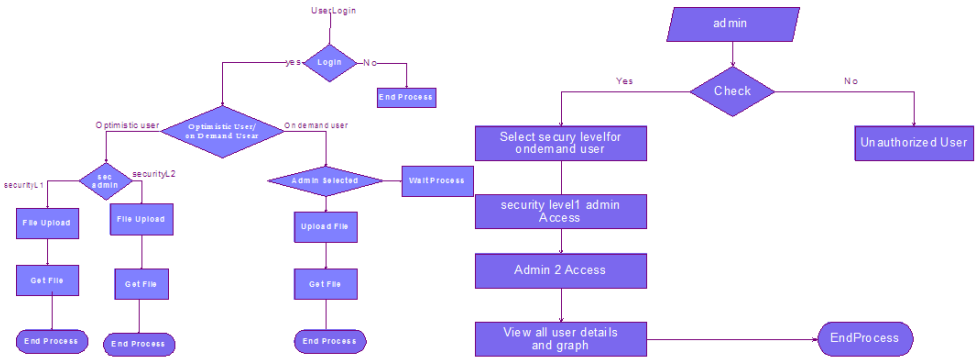


Figure 2. Authentication Process

3. Related Work

Authentication is necessary for cloud especially the more efficient and lightweight user side to outsource their computation tasks. Authentication for cloud and traditional web environment is widely adopted the use of Identity Based Authentication [5], R.A. Popa et.al [13] and many other devoted frameworks [7] which uses security key to allow users verify their identity to the authentication server according to their security requirements. However, this architecture is not ready for deployment in practical applications yet access

control in traditional web applications and Cloud services is different from cloud environment usage.

Schemes provided by C.Gentry [6] and O. Goldreich [18] solving a central open problem in cryptography allows one to compute arbitrary functions over encrypted data without the decryption key as fully homomorphic encryption schemes are not yet sufficiently fast enough for evaluating a large functionality such as a garbled circuit under fully homomorphic encryption and externalizes access control form web applications.

P. Jagadpramana et al [8] provide a framework for the tracking and auditing of the file access history and data provenance. This policy management as a Service in Cloud management will empower service providers and users to reduce Top Threats to Cloud Computing Report (Ver.1.0). As such, our work provides transparency that identifies trust via public auditing of the file access history and users can be able monitor the system event logs of the services they engage.

The requirements and access control rules for Robe-Based Access Control (RBAC) common definition meeting the secure processing needs is described in [10]. In this model access control based on user roles could be used as the basis starting common ground for RBAC provide a means of naming and describing relationships between individuals and rights, providing a method of meeting the secure processing needs of many individuals and industries. Framework provided by D. Richard Kuhn et.al [11] externalizes access control form permission constraints and provide it in form of role-centric RBAC-A scheme requires changing the RBAC standard to constrain the set of permissions available during a user's session. Attribute Based Access Control (ABAC) and Role Based Access Control (RBAC) are merged and named as RBAC-A.It provides access controls thus enhancing the security needed for a private Cloud which are implemented by the server side. Our designed system is efficient so it provides optimize access control services to mobile users in Cloud environment and level of security is achieved by incorporating trust (public auditing) into Access Control for Cloud environment, hence incorporating users to specify theirs access control requirements according to their own security needs.

A scalable access control system for encrypted data is designed in [15] for a public Cloud. A hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a cipher text-policy attribute-based encryption (CP-ABE) system, so as to provide not only fine-rained access control, but also full delegation and high performance. So as to efficiently revoke access rights from users. Access control based on encryption (selective encryption) is presented in [14]. The authors mentioned that focus is the presentation of experimental results to demonstrate the applicability of their proposal, that implies sort of authorization can dynamically change. In such scenarios the set of keys withheld by each user involved in the changes may to be subjected to update and re-encrypt. Another access control model for cloud environment is described in [16] based on encrypted queries on encrypted of data and do not require re-distributing keys or re-encryption of data. A proposed architecture provided by L. Ferretti et.al [12] guarantees confidentiality of data stored in public database on encrypted data and does not require modifications to the cloud database with implies no access control. The focus of the above mentioned solutions is to achieve high level of security through enhanced access control models which are implemented by the server side. None of these models are security based choice from end users (the on-demand users and optimistic users) access the cloud space in secure manner. While our approach also does not imply sort of authorization and cloud admin only provide security on cloud, more security into user's data against insecure remote data storage (cloud) but not have access to user's data.

4. Protocol Statement

The proposed protocol consists of three conceptual steps for users access cloud space (storage) which are: (1) Registration –all cloud user are registered and select user-type (on demand users or optimistic users) and User Login to authenticate themselves by providing their Username, Password and User Type, (2) Access control based on user types, (3) Accessing protected resource storage usually at Administrative Management Domain (ADMD) level, (4) File Size Usage of Cloud Space Analysis.

A. Authentication Process

Here the first step for the user to access cloud space is to register provide their credential (such as Email, User Type (select user type: On-demand users or optimistic user), Username and password) which are stored in the public cloud database that allows user to access all and only legitimate roles. As shown in figure 2 user has to provide his/her username, password, select User type (on-demand or optimistic) and authenticated by logging to access the services in cloud space. After user authenticated by logging to access cloud space the cloud admin permit user with access to the request, checks user defined policies by evaluating the request against them and generates the decision only provide on-demand user access security level. Hence, provides user with the access to its account on the cloud services. The cloud admin will permit user with access to the cloud space and on selection of security level depending on user-type. Cloud admin permit On-Demand User Access to security Level and user can have access to upload file, send cloud, and downloading file are the only roles that have access to all user registered to access cloud space application.

B. Access Control Process for Security to Access Cloud Space

Before an authenticated user interact with any services in the cloud space, cloud admin does the role to permit access to the services by assigning security level to different cloud user types on cloud environment usage, and security level are different to both end users. After getting access to the cloud space services, the user have a privilege to the services by employing it for example if a user choose to upload the file, can browse the file from the directory of their devices and upload it into the application, and user have to assign the File_Name for the corresponding uploaded file. After uploading the file a prompt window will appear which require user to select encryption algorithms and the uploaded file will be encrypted in file encrypt storage form and finally file will be successful uploaded stored in public database in encrypted form. While only legitimate roles into this application are upload, send to cloud, packet sending, and download file to access cloud space.

(a)File Upload with Security Level 1 (b) File Download with Security Level 1

(c)File Upload with Security Level 2 (d) File Download with Security Level 2

Figure 3. File Upload/Download Window Prompt

The next thing user have to do is send the file to the cloud (send to cloud), and user have to monitor its status which is defines access control with an interface which resides in the user's devices. Before, user finally completed send uploaded file to a cloud, a prompt window will appear that require user to provide Keyword with upload the security key for cloud for intended file to be sent to a cloud space. After upload the security key for cloud, and success send it to a cloud, user has to wait (defines access control on it) for conformation for permission from cloud admin, in this case could determine a full legitimate for user to access the cloud space, and to her/his file uploaded or having want access of downloading the file in this cloud application. After cloud admin take administrative action defines access control to accept user send cloud file, user can have a legitimate to search a file using File_Name, and the application will prompt the Access Key of the user uploaded securing key to the cloud during file upload session.

User has to click once again on search button in the application, prompt a window contains field column of encrypted file, algorithm, own user Access Key, and Admin send Key Mail Access Key. As shown in the Figure 3(b). User has to select/upload algorithm again, input his/her own Access Key created early during file upload session, and input Admin send Key Mail Access Key sent to her/him by cloud admin to his/her original registered email accounts. Hence user will be able to download and access the file otherwise not correct algorithm and access key cloud can prompt an error window for user has to select algorithm and access key again or won't be able to download file as shown in figure 3(b) ,while the figure 4 illustrates the steps of this process.

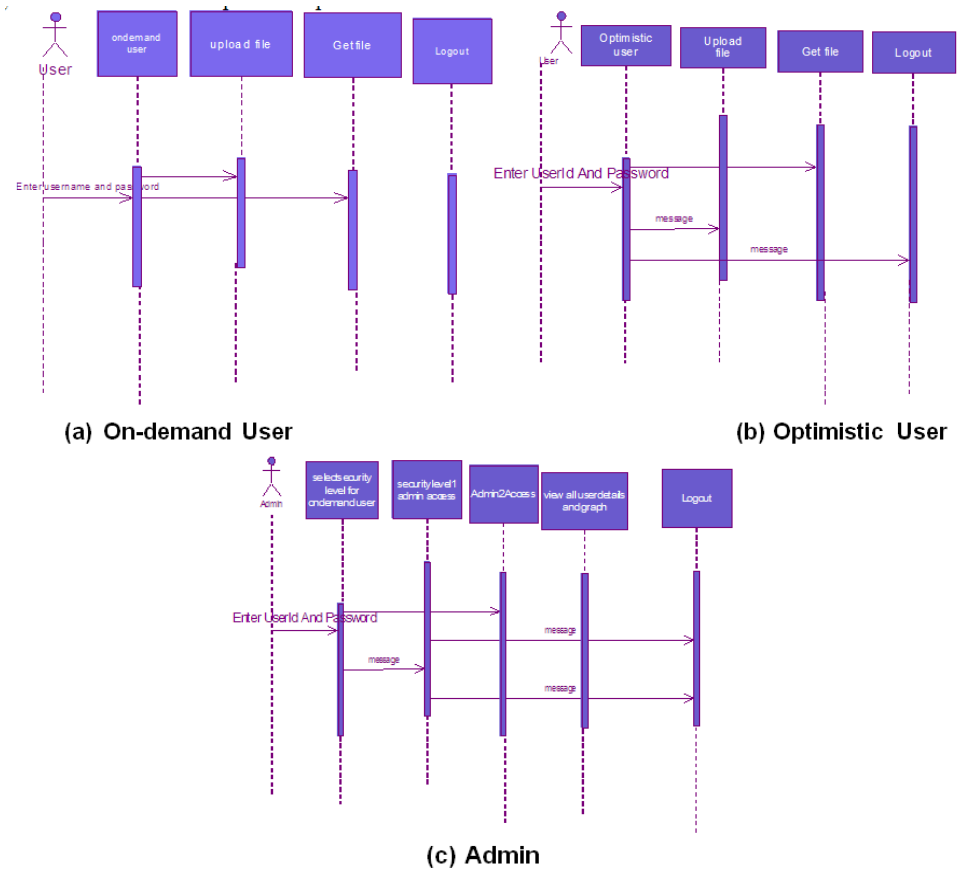
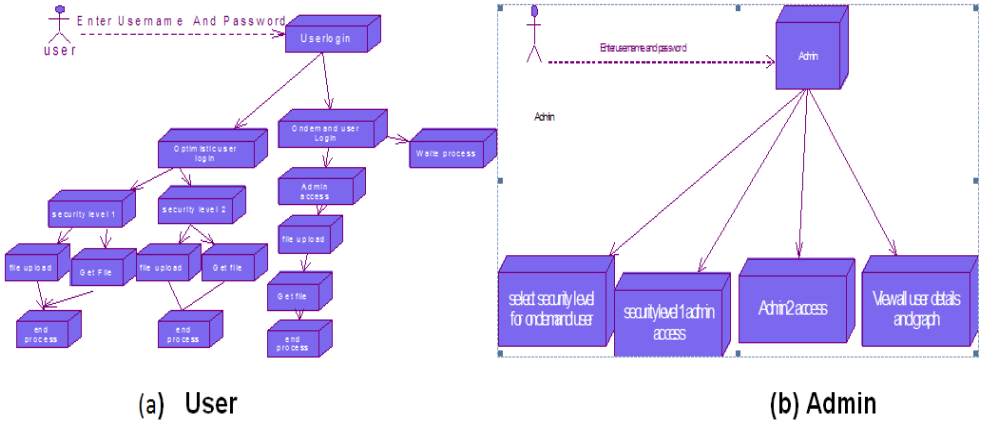


Figure 4. Access Control Process

C. Accessing Protected Resource Storage and Transfer Message

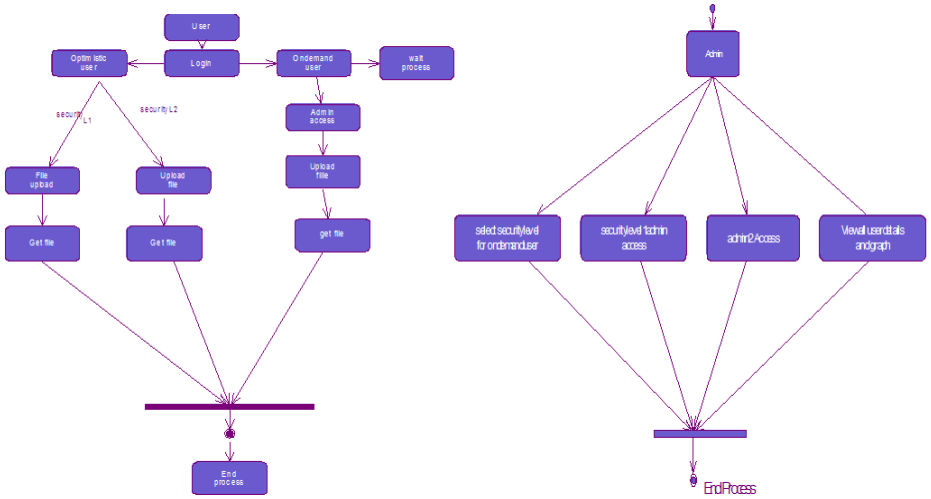
In this step registered user access uploaded file stored in cloud space in file storage encrypt format. To guarantee file confidentiality a combined selective encryption

algorithm over an uploaded file is uploaded (input) to ensure the security of the transfer message within the environment between these two parties. The access request contains the unknown part that time only get full data, the cloud server checks the user defined access control for the particular service and an access request generates the File Storage Block Format.



(a) User (b) Admin

Figure 5. Accessing Protected Service Storage and Transfer Message



(a) User **(b) Admin**

Figure 6. Activity Diagram

When a user security part is unknown can access the cloud space, if the unknown part upload file and send packet. The defined access control prompts Three File Block Password Format which needs to be input any keyword to generate proof key that could be used in case the unknown part need to download the file. Cloud admin evaluate the request against them, and permit the access or otherwise. On which the user access control for security defined, Upload file and sending packet of the uploaded file set the file to be stored in a File Storage Block Format because of security to detect loss and to protect against attackers both in insufficient transport layer protection and insecure remote data storage. As shown in figure 5 illustrates User-Types access cloud space hosts different services that is the application for the storage and management the access control for security of the encrypted file.

D. File Size Usage of Cloud Space Analysis

These charts are representing the usage of cloud space and depend upon the types of users in cloud.Based on the cloud user type the security will be changed over the cloud. As illustrated in figure 7 and 8, X-axis represents the File Name (list of files for particular user) and y-axis represents the Size of the file (file_Size).

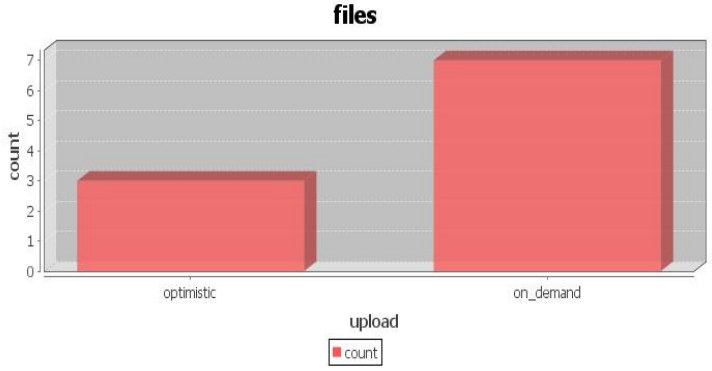
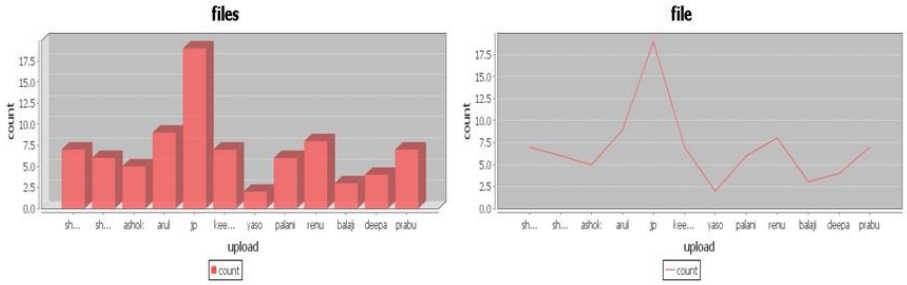


Figure 7. File Size Usage Based on the Cloud User Type



(a) **(b)**

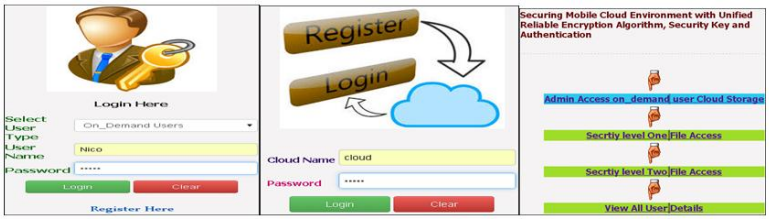
Figure 8. Histogram and Line Chart of File Size Usage of Cloud Space

5. Analysis System Design Scenario

As shown in figure 6 activity diagram and these stages can be illustrated in figure 9. This section present a simple analyzes of the scenario which describes the functionality and applicability of the employment for the designed application system. The designed application system scenario comprises of user who wants use this application simply by positing and storing her/his data into cloud space. The following provide and describe the steps of the designed system scenario in detail:

- Firstly user registers herself/himself to get user credentials (i.e. User-Type, Username and Password) which provide user legitimate to authenticate by login into the application as shown in figure 9(a).
- After user logged in the application different services of each role are provided with different access control for security.
- If which ever User-Type (on-demand user or optimistic user) need to employ any role (such as upload, send to cloud, download file) within the application the defined access control for security for the particular service requested will be stored and transfer message in encrypted form or in a storage block form between these two parties.
- For the particular service requested by the user defined access control for security requires user create/input keyword to generate a proof key and select security level (that is optimistic user), for on-demand user a (pre)-defined security level will be provided by a cloud admin and await access permit.

- A cloud admin will checks evaluate the service request and permit access or otherwise as shown in figure 9(c).
- Then user wants to access the file she/he uploaded and send to the cloud. A cloud admin will send email on original user register mail with access key along with File_Name only of the file user requested to access to.



(a) User Login **(b) Admin Login Access** **(c) Public Audit/Security**

Figure 9. Security Level Access Control and Public Auditing for End-User

The above scenario literature described using authentication mechanisms and access control to the resources/services with the user account at fine level granularly for simplicity and better understanding. User can have access to different services which are been given in a different way with different security level that associated with user account. The detailed of the designed system of application for access control introduce the database models and mechanisms for combining encryption algorithm and for metadata to ensure data confidentiality. The server makes some decision using the security specification with a unified defined access control over its services hosted on cloud space. Encrypting file will protect user against this scenario and cloud admin won't have user's access.

6. Conclusions and Future Work

In this project the end user access the cloud space in secure manner but the security is varying for both the on-demand users and optimistic users. The services are also different from both types of the cloud users. The on-demand users are getting the cloud environment usage in long period of time. They have to maintain the data also in a secure manner and cost for the on-demand users are also high. But the optimistic users use the cloud environment in short period of time and also security is also less compared to the on-demand users. In our future work the utilization of cloud is very easily and securely at optimistic user also but they have to get the access control for security .Cloud environment usage for on-demand users and optimistic users are different. The security provision is also different from both users. On-demand users are having more sufficient provisions security compared to optimistic users. In future we have to give the required security for optimistic users also but optimistic users are getting an access control for security in another way due to the defined security. On the other hand, it's different from cloud environment usage and storage.

Acknowledgements

This work was partially supported by the NSF of China under grants No. 61173048 and No. 61300041, Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 20130074110015, and the Fundamental Research Funds for the Central Universities under Grant No.WH1314038.

References

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing,Ottawa,ON, (**2012**), pp. 556–563.
[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Services Computing, vol. 5, issue. 2, (**2012**), pp. 220–232.
[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren and W. Lou, "Fuzzy keyword Search over Encrypted Data in Cloud Computing," in IEEE INFOCOM, (**2010**), pp. 441–445.
[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054, (**2010**), pp. 136–149, Springer.
[5] H. Li, Y. Dai, L. Tian and H. Yang, "Identity-Based Authentication for Cloud Computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931, (**2009**), pp. 157-166, Springer.
[6] C. Gentry, "A fully Homomorphic Encryption Scheme," Ph.D. dissertation, Stanford University, (**2009**), http://www.crypto.stanford.edu/craig.
[7] A. -R. Sadeghi, T. Schneider and M. Winandy, "Token-Based Cloud Computing", in TRUST, ser. Lecture Notes in Computer Science, vol. 6101, (**2010**), pp. 417–429, Springer.
[8] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang and B. S. Lee, "Trustcloud, A Framework for Accountability andTtrust in Cloud Computing", HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.
[9] R. Lu, X. Lin, X. Liang and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", in ACM ASIACCS, (**2010**), pp. 282–292.
[10] D. F. Ferraiolo and D. R. Kuhn, "Role-Based Access Controls," in 15th National Computer Security Conference, (**1992**).
[11] D. R. Kuhn, E. J. Coyne and T. R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, (**2010**), pp. 79–81.
[12] L. Ferretti, M. Colajanni and M. Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, (**2014**), pp. 437–446.
[13] R. A. Popa, C. M. S. Redfield, N. Zeldovich and H. Balakrishnan, "CryptDB, Protecting Confidentiality with Encrypted Query Processing," in Proc. 23rd ACM Symp. Operating Systems Principles, (**2011**) October, pp. 85–100.
[14] E. Damiani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, "Key Management for Multi-User Encrypted Databases," in Proc. ACM Workshop Storage Security and Survivability, (**2005**) November, pp. 74 – 83.
[15] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical Attribute-Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers", Computers & Security, vol. 30, no. 5, (**2011**), pp. 320–331.
[16] M. R. Asghar, G. Russello, B. Crispo and M. Ion, "Supporting Complex Queries and Access Policies for Multi-User Encrypted Databases", in Proc. 2013 ACM Workshop on Cloud computing security, (**2013**) November, pp. 77–88.
[17] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak and M. Bowman, "Planetlab, An Overlay Testbed for Broad Coverage Services", ACM SIGCOMM Computer Communication Review, vol. 33, no. 3, (**2003**), pp. 3–12.
[18] O. Goldreich, "Foundations of Cryptography Volume 2, Basic Applications", Cambridge university press, (**2004**).

Authors

Buchanagandi E Nyamajeje, he has master's degree in Information Science and Engineering from East China University of Science and Technology. Currently, he pursues PhD in computer science and engineering. His resaerch interests are mobile multimedia and cloud computing, software enginering.

Huiqun Yu, he has doctoral degree in computer science from Shanghai Jiaotong University. He is Dean at East China University of Sci. and Tech., Dept. of Computer Science and Engineering. He is IEEE Senior Member and reviewer for International Journal of Computers and Applications, International Journal of Software Engineering and Knowledge Engineering. His research interests are Software Engineering, High Confidence Computing Systems, *etc*.