ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 12 , December 2017

Cryptographic System assisted Secure Cloud Storage Systems

Asutosh Hota, Sai Sankar Gochhayat, Mohit Nayak,Manoranjan Panda

U.G. Student, Department of Computer Science and Engineering,College of Engineering and Technology, Bhubaneswar, India

U.G. Student, Department of Computer Science and Engineering,College of Engineering and Technology, Bhubaneswar, India

U.G. Student, Department of Instrumentation and Electronics, College of Engineering and Technology, Bhubaneswar, India

Lecturer, Department of Computer Science and Engineering, College of Engineering and Technology, Bhubaneswar, India

ABSTRACT: This paper derives the possibilities of establishing a Secure Cloud Storages System (SCSS) is proposed that comprises of effective, light weight secure storage system with RSA and AES algorithm and prevents unauthorized access and modification of stored data through security policies. Cloud computing provides Cloud storage as a service to the users for hosting their data in the cloud. Secure data storage is required as the data is outsourced to external storage and Data access control is the well-organized method to provide data security in cloud. Trust based data upload rights are provided to the users which improves security. The existing Cipher text-Policy Attribute-based Encryption (CP-ABE) is difficult to apply in multi authority cloud storage due to the attribute revocation problem. This paper proposes a revocable multi-authority CP-ABE scheme thus, providing solution to the role revocation problem. The proposed scheme updates the components of the revoked role only and generates latest secret keys for the revoked role and forwards it to the non-revoked users who have the rolesCloud Computing, Advanced Encryption Standard(AES), CP-ABE, RSA as revoked roles hence assuring backward security and Forward security.

KEYWORDS: Cloud Computing, Advanced Encryption Standard (AES), CP-ABE, RSA

I.INTRODUCTION

Multi-authority CP-ABE is mostly considered technology for data access control in cloud storage systems. Users may hold various roles issued by multiple authorities. The data access policy over the role is defined by the authorities and not by the data owners. The existing system is not applicable for multi-authority cloud storage due to its role revocation problem. If any role is revoked means all the Cipher text associated with the authority whose role is revoked should be replaced or updated. The existing system relies on a trusted server. The data hosting and data access in cloud initiate a challenge in data access control. The cloud servers cannot be fully trusted by data owners; they cannot be able to rely on servers to do access control. The data owners cannot be able to assign the data access policies for the users according to their role relationship. In multi-authority cloud storage systems, user's roles can be changed dynamically. A user may have new role generated by several other authorities and the user may revoke some of the current roles. The user's data accessing permission should be changed accordingly with the dynamic adoption of new role entitling and role revocation. Secure data storage is required as the data is outsourced to external storage and Data access control is the well-organized method to provide data security in cloud. A Secure Cloud Storages System (SCSS) is proposed that comprises of effective, light weight secure storage system with RSA and AES algorithm and prevents unauthorized access and modification of stored data through security policies. Trust based data upload rights are provided to the users which improves security. The existing Ciphertext-Policy Attribute-based Encryption (CP-ABE) is difficult to apply in multi authority cloud storage due to the attribute revocation problem. The proposed revocable multi-authority CP-ABE scheme provides solution to the role revocation problem. The proposed scheme updates the components of the revoked role only and generates latest secret keys for the revoked role and forwards it to the non-revoked users who have the roles as revoked roles. The backward security and Forward security is assured. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself. The major contribution to the paper would be to propose a lightweight

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 12 , December 2017

cost effective secure cloud storage and access control system. The major aim would be to solve the role revocation problem in multi-authority cloud storage and provide both the Backward security and Forward security
The global authority is separated into Administrator (AD) and Role Manager (RM).RM combines the global public key and public key generated by AD for generating the secret key. Only the components associated with the revoked role is updated and no need to update all the role components The Cipher text updating in cloud enables the Forward Security All the users are need to hold only the latest secret key, no need to keep records on the previous secret keys. The revoked user can access the system after doing the registration process again and get the access according to access control policy. After registration the revoked user may try to access the system using his/her old authentication details. Therefore, the authentication details of each and every user involved in the system are stored separately. The unique identity of the user such as Social Security Number (SSN)/ General Identity card number is added in the revocation list. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself. There is the possibility for the revoked user or external attacker to hack the token of the existing user from the database of the cloud and access the stored data using the hacked token. To prevent from such vulnerability, hash value of the token corresponding to each user is stored in the database instead of direct token itself. Whenever user enters into the system with token, authentication is done as follows: Hash value of the token is calculated and it is matched with the stored hash value in the database. If it is matched, they are authenticated user else their access is denied.

II.RELATED WORK

The work in the field of establishing the best practices for achieving a secured cloud system has been tremendous and with the advancements in the field of high computational and decreased processing time, the systems of the present are now equipped with better performances with computability, security and network stability. The work [13] focused on multiple security domains and thus reducing the key management complexity for the user as well as the owners. A high degree of patient privacy is guaranteed by exploiting multi-authority ABE framework. It addresses the unique challenges brought by multiple owners and users. [14] provides a trade off in terms of efficiency and complexity of assumptions. It achieved analogous expressiveness and efficiency to the Goyal construction, but in the Cipher text-Policy ABE setting. However, parameter was limited to a proof in the generic group model and problem of finding an expressive CP-ABE system under a more solid model was needed. Work in the key extraction concepts like [15] has devised efficient methods to permit adaptive pirates to be traced and thus, construct a scheme which allows a greater number of key extraction queries by the pirate than ours allows. Furthermore, the key leakage problem in the settings of multi-authority ABE was alleviated. In [16], the system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. It included several optimization techniques. The sensitive data has been stored n encrypted form. Work in Key-Policy ABE and Cipher text-Policy ABE has been prevailed for long and many researchers have meticulously laid important foundations to the same. [17] establishes an attribute-based encryption system with different types of express. Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys. While in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Similar systems have been established by [18] which allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. The set of attributes allowed in each clause must be disjoint.

III. PROPOSED SYSTEM

The components of SCSS system is separated into Administrator (AD) and Role Manager (RM). The AD sets up the system and registration of each user and RM is done. The AD provides unique identity to each user and unique identity to each RM. Role Manager only generates the secret keys for the role and forward it to the user. Each RM generates global public key. It combines the global public key and public key generated by AD for generating the secret key. The data owners first split the data into multiple components according to logical granularities and design an access policy for each role. The data owner encrypts the data with content keys using symmetric encryption algorithm. Then the content keys are encrypted based on access policies of each role and send the encrypted data together with Cipher texts to the cloud. Users are allowed only to download the data from the cloud. Uploading rights are provided to the users by the AD and data owner if their trust reaches the threshold. When a role of the user is revoked, only those components associated with the revoked role in secret keys and Cipher texts need to be updated. The RM generates a new version number for the revoked role and generates an update key. By using the update key, the components associated with the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 12 , December 2017

revoked role in the Cipher text can also be updated to the current version. The corresponding updated Cipher texts in cloud also updated. The global authority is separated into Administrator (AD) and Role Manager (RM). RM combines the global public key and public key generated by AD for generating the secret key. Only the components associated with the revoked role is updated and no need to update all the role components. The Cipher text updating in cloud enables the Forward Security All the users are need to hold only the latest secret key, no need to keep records on the previous secret keys.

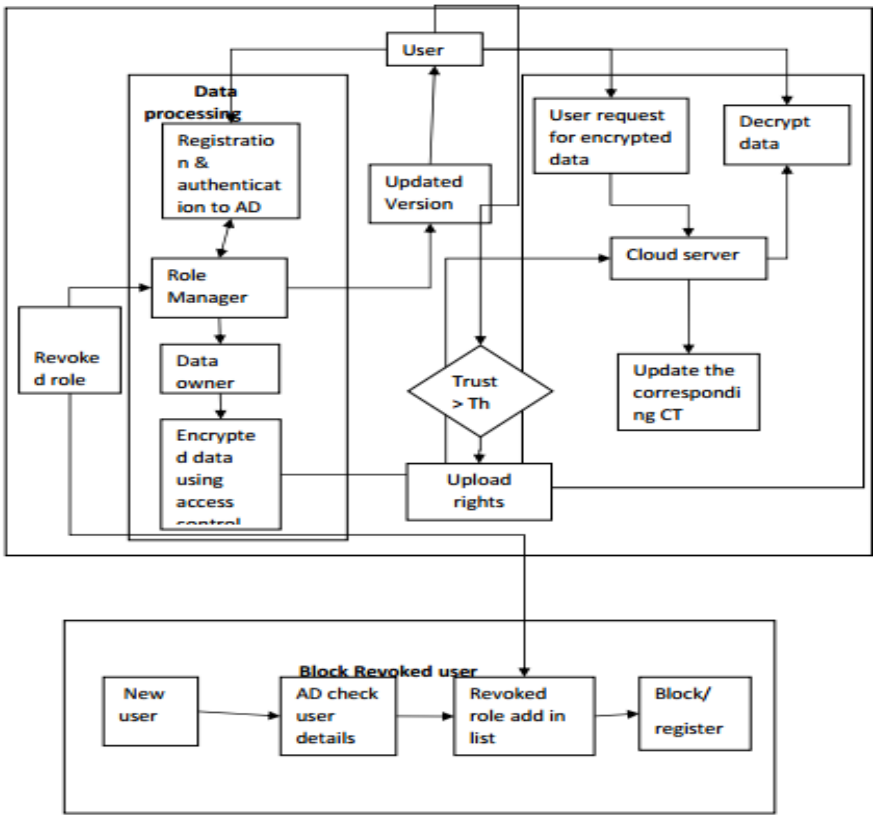

Fig. 1. Block diagram for the proposed system

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 12 , December 2017

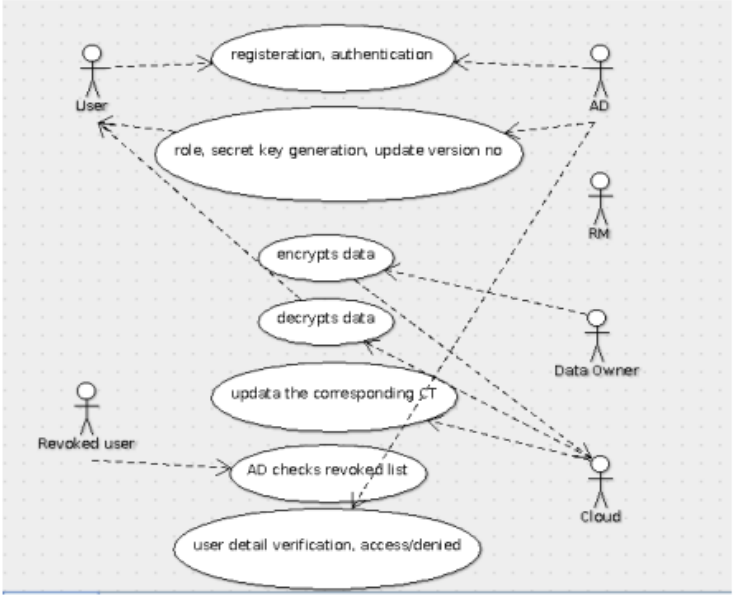

Fig. 2. Use case diagram for the system workflow

IV. SIMULATION TEST BED AND CLOUDSIM

CloudSim a new, generalized, and extensible simulation framework that allows seamless modelling, simulation, and experimentation of emerging Cloud computing infrastructures and application services. By using CloudSim, researchers and industry based developers can test the performance of a newly developed application service in a controlled and easy to set-up environment. Based on the evaluation results reported by CloudSim, they can further finetune the service performance. The main advantages of using CloudSim for initial performance testing include: (i)time effectiveness: it requires very less effort and time to implement Cloud-based application provisioning test environment and (ii) flexibility and applicability: developers can model and test the performance of their application services in heterogeneous Cloud environments (Amazon EC2, Microsoft Azure) with little programming and deployment effort. CloudSim offers the following novel features:
(i) Support for modelling and simulation of large scale Cloud computing environments, including data centers, on a single physical computing node;
(ii) a self-contained platform for modelling Clouds, service brokers, provisioning, and allocation policies;
(iii) Support for simulation of network connections among the simulated system elements; and
(iv) facility for simulation of federated Cloud environment that inter-networks resources from both private and public domains, a feature critical for research studies related to Cloud-Bursts and automatic application scaling.
Some of the unique features of CloudSim are:
(i) availability of a virtualization engine that aids in the creation and management of multiple, independent, and co-hosted virtualized services on a data center node and
(ii) Flexibility to switch between space-shared and time-shared allocation of processing cores to virtualized services. These compelling features of CloudSim would speed up the development of new application provisioning algorithms for Cloud computing.

A. Cloudsim Architecture

The following figure shows the layered implementation of the CloudSim software framework and architectural components. At the lowest layer is the SimJava discrete event simulation engine [6] that implements the core functionalities required for higher level simulation frameworks such as queuing and processing of events, creation of system components (services, host, data center, broker, virtual machines), communication between components, and management of the simulation clock. The top-most layer in the simulation stack is the User Code that exposes configuration related functionalities for hosts (number of machines, their specification and so on), applications (number

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 12 , December 2017

of tasks and their requirements), VMs, number of users and their application types, and broker scheduling policies. A Cloud application developer can generate a mix of user request distributions, application configurations, and Cloud availability scenarios at this layer and perform robust tests based on the custom Cloud configurations already supported within the CloudSim. As Cloud computing is a rapidly evolving research area, there is a severe lack of defined standards, tools and methods that can efficiently tackle the infrastructure and application level complexities. Hence in the near future there would be a number of research efforts both in academia and industry towards defining core algorithms, policies, application benchmarking based on execution contexts. By extending the basic functionalities already exposed by CloudSim, researchers would be able to perform tests based on specific scenarios and configurations.

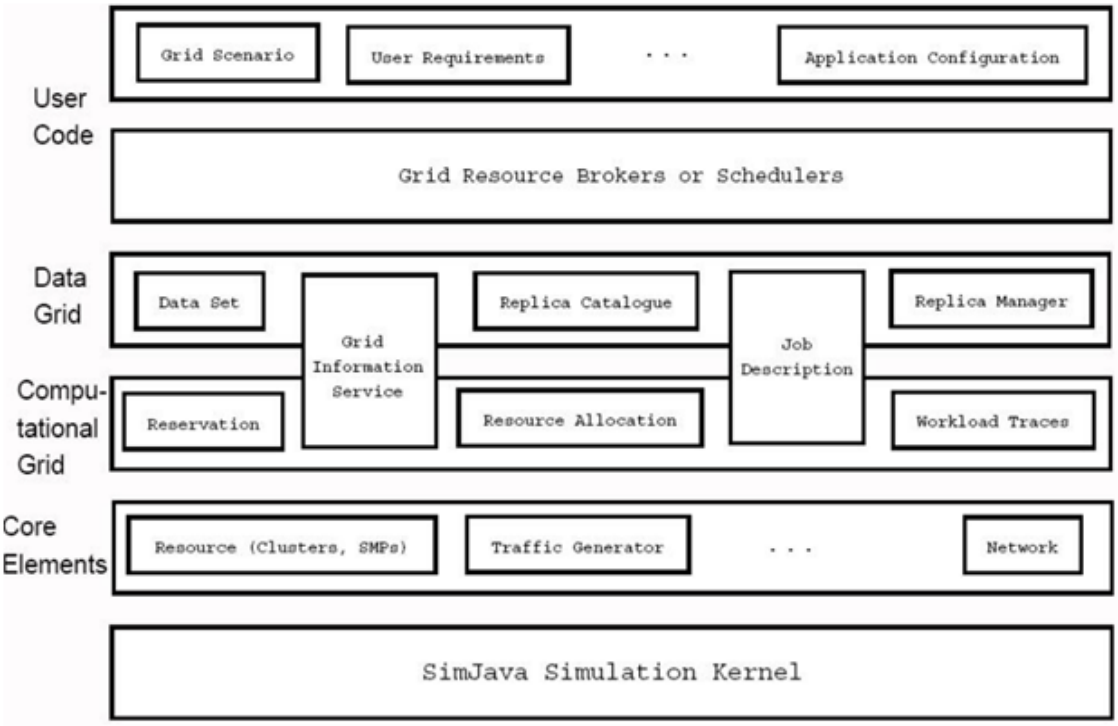

Fig. 3. Architecture of CloudSim 3.0.3

B. Hardware and software specifications

Table. 1. Hardware and software specifications for the testing bed.

Sl. No.	Name	Specifications
Hardware		
1	Processor	Pentium Dual core @ 3.20GHz.
2	RAM	4 GB of RAM
Software		
1	Languages	Java JDK 1.8
2	Operating System	Windows/Ubuntu 14.04
3	Front End	Java Swing
4	Backend	MySQL
5	Framework	CloudSim 3.0.3
6	IDE	Netbeans 8.0

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 12 , December 2017

C. Results and Performance analysis

The following figures [Fig.8 – Fig.10] would explain the process of the whole proposed system with a step by step detailed view and workflow.

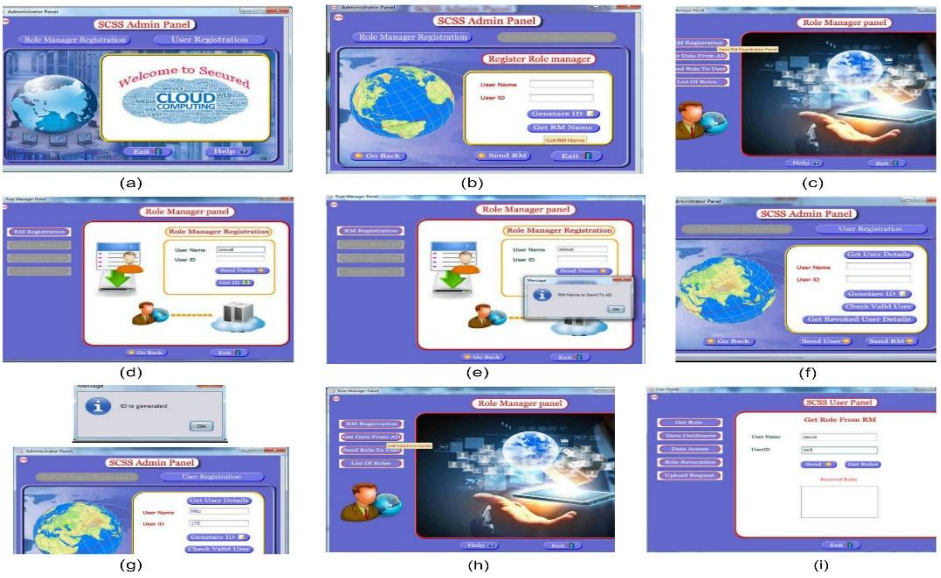

Fig. 4. (a) Admin Panel, **(b)** Register role manager**,(c)** Role manager panel, **(d)** Role manager registration, **(e)** RM name is registered and sent to AD, **(f)** User registration panel: This panel not only receives the name of user but also authenticates and validates the user based on the roles and creates Keys for valid users, **(g)** unique ID and a unique Hash code will be generated for the new user. Hash code is stored in Hash code table of Database for Admin authentication purpose and ID will be sent to the user for future login, **(h)** Role Manager panel, **(i**) The register details of the user will be reflected in the RM panel. On clicking OK, Now the user details will be stored in the Role table of database.

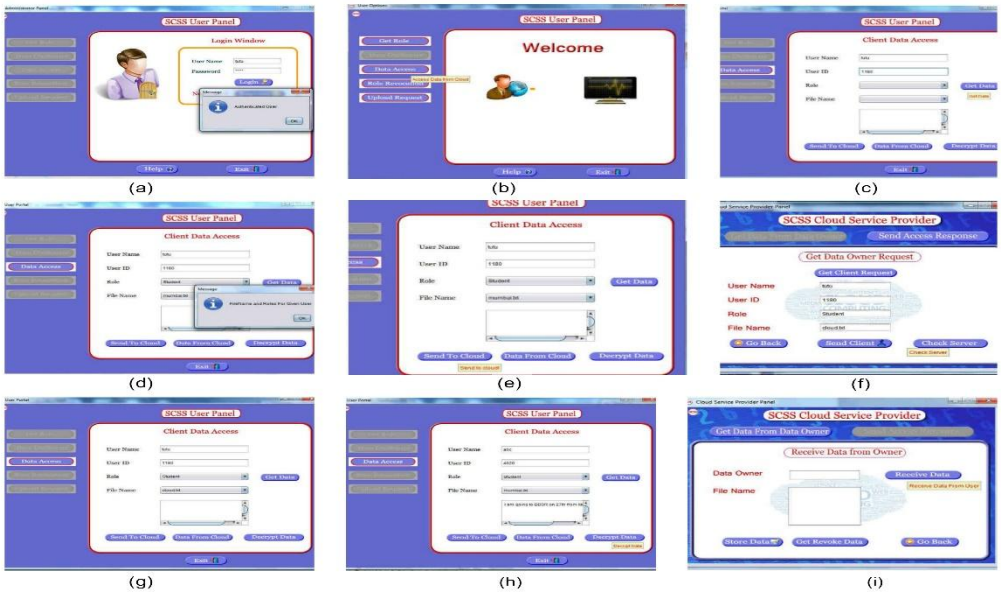

Fig. 5. (a) Authentication of existing user, **(b)** Upload request button**, (c)** Client data access, **(d)** Role assignment and evoking, **(e)** Data will be reflected in the cloud panel and received data from data owner will be displayed, **(f)** Data to be sent to cloud, **(g)** Data access from cloud, **(h)** Client access control, **(i)** Receive data from cloud

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 12 , December 2017

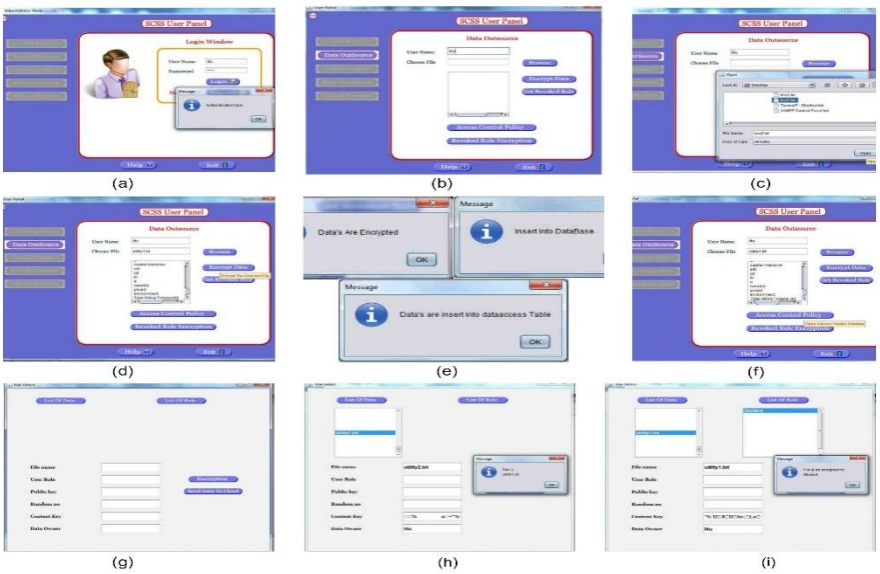

Fig. 6. (a) Login User and select Data Outsource button, **(b)** Data outsource and file upload, **(c)** Uploading files to outsource, **(d)** Encrypt the selected data, **(e**) Confirmation for data encryption and upload, **(f)** Access control policy window, **(g**) Role details**, (h)** Configuring access policy details, **(i)** File is assigned.

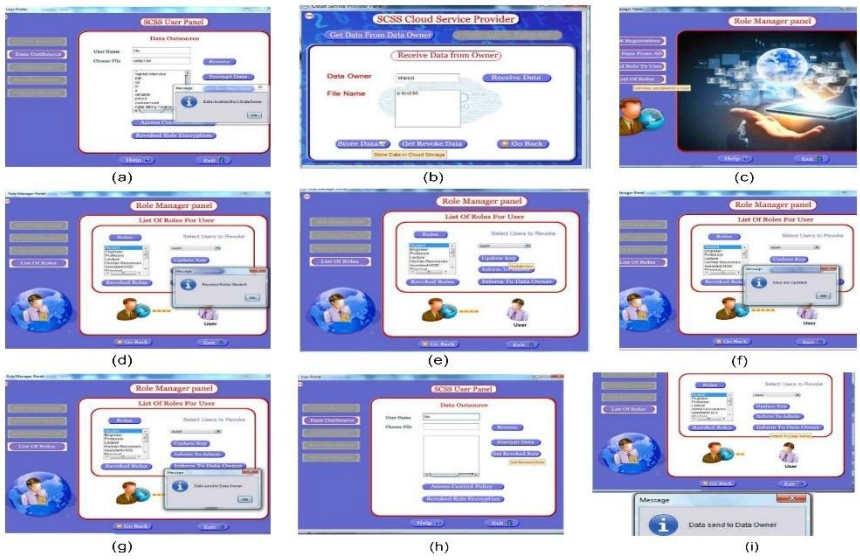

Fig. 6. (a) Cloud owner name and file name fields will be filled to confirm receive of data, **(b)** Data received from owner and accessed, **(c)** RM panel and select roles from list, **(d)** Revoking role from list, **(e**) key update for data encryption and upload, **(f)** keys are updated and role has been revoked, **(g**) Data sent to inform admin button**, (h)** Data outsourcing and control access policy **(i)** Data has been sent to the data owner.

V. CONCLUSION

A revocable multi-authority SCSS scheme can support efficient role revocation. We constructed an effective data access control and secure storage scheme for multi-authority cloud storage systems. It is a promising technique, which can be applied in any remote storage systems and online social networks etc. It will provide security to the data from unauthorized access and eavesdropping. If any hacker will try to register with a revoked user role it will be simply denied by the system. Hence cloud data will be safer.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 12 , December 2017

REFERENCES

[1] BokefodeJayant D, UbaleSwapnajaA,PringaleSubhashV,KarandeKailashJ,ApateSulabha S. "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model"
[2] Solapur University,India,12 May 2015.
[3] Y. Deswarte, L. Blain, and J.-C. Fabre, "Intrusion Tolerance in Distributed Computing Systems," Proc. Symp. Research in Security and Privacy, pp. 110-121, May 1991.
[4] Encyclopedia of Cryptography and Security, Henk C A van Tilborg , Eindhoven University of Technology, The Netherlands
[5] http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf
[6] http://www.buyya.com/papers/CloudSim2010.pdf
[7] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009, pp. 121-130.
[8] Mohammed E.M. , Ambelkadar H.S, Enhanced Data Security Model on Cloud Computing, In Proc. 8th International Conference on IEEE publication 2012,pp.12-17
[9] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.
[10] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''Scalable and SecureSharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.
[11] J. Hur and D.K. Noh, ''Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221,July 2011.
[12] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.
[13] Bharti RatanMadnani , Sreedevi N , "Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013
[14] Brent Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization."
[15] MA Haiying, Guosun ZENG, Zhanjun WANG, and Jinchao XU, "Fully Secure Multi-authority Attribute-based Traitor Tracingど ,". Journal of Computational Information Systems 9, no. 7, pp.2793-2800,2013
[16] John Bethen court, Amit Sahai, "Cipher text-Policy Attribute-Based Encryption", IEEE Symposium on Security and Priivacy, 2007
[17] Sonia Jahid, Prateek Mittal, Nikita Borisov, "EASIER: Encryption-based Access Control in Social Networks with Efficient Revocation",6th ACM Symposium on Information, Computer and Communications Security , March 22 - 24, 2011
[18] Melissa Chase, "Multi-Authority Attribute Based Encryption", TCC'07 Proceedings of the 4th conference on Theory of cryptography,2007