REVIEW OF RESEARCH
IMPACT FACTOR : 5.7631(UIF) UGC APPROVED JOURNAL NO. 48514 ISSN: 2249-894X
VOLUME - 7 | ISSUE - 12 | SEPTEMBER - 2018

ENHANCING THE SECURITY OF DATA IN MOBILE CLOUD COMPUTING

Prof. V. Sangeetha[1] and D. Jagadeeshwari[2]
[1]M.Sc., M.Phil., SET., B.Ed., Head, PG and Research Department of Computer Science.
[2]M.Phil., Research Scholor, PG and Research Department of Computer Science, Sri Bharathi Women's Arts and Science College, Kunnathur, Arni, T V Malai Dt.

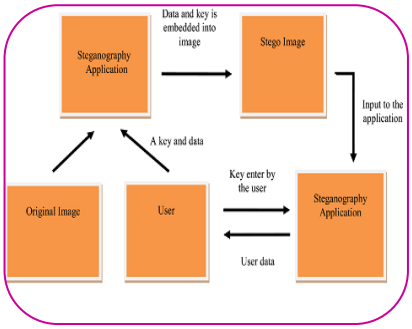
ABSTRACT:

Now a day's smart mobile devices are deployed with different cloud based services like Google applications, Instagram, Facebook etc., which have been widely developed as mobile applications for mobile cloud computing. The latest hardware and programming developments in smart gadgets has given give consistent collaboration between the clients and devices. Thus, rather than the conventional user, the mobile client in mobile Cloud environment creates an expansive volume of information which can be effectively gathered by mobile Cloud service providers. Moreover, the mobile users don't have the precise thought regarding the positive physical area of their own data. Along these lines, the users can't control over their data once it is put away in the Cloud. This thesis examines security and protection issues in such mobile Cloud environments and exhibits new client driven access control systems customized for the versatile Cloud situations. With a particular final objective to organize the data security and client's assurance in mobile cloud environment, the thesis investigates Cipher Text - Attribute-based encryption (CP-ABE) strategies in mobile cloud computing. CP-ABE plan empowers information owners to authorize access arrangements amid the encryption. Connection related attributes, for example, requester's area and conduct are consolidated within ABE plan to give information on security and client protection. This will enable the owners of the mobile data to logically control the passage to their data at runtime. Remembering the final objective to improve the execution, an answer that offloads the high-cost computational work and interchanges from the smart devices to the Cloud is proposed. Secret methods are integrated in the key issuing protocol so that the user's identities are shielded from being followed by the service providers amid information exchanges. The proposed plans are secure from known attacks and thus suitable for mobile Cloud environment. Implementations of the proposed plans are formally scrutinized utilizing standard techniques on mobile and cloud environment.

KEYWORDS: *RSA Algorithm, DES Algorithm, Multi-cloud, ECC Algorithm* .

INTRODUCTION

Advances in the field of Information Technology has influenced outsourcing of information and sharing. Social networking websites and e-documents offer an easy method for users to outsource and share diverse information on the cloud storage servers such as photos, events, news, etc. Cloud Computing arises to be the future of IT architecture, thus it provides unlimited and flexible resource for storage in cost efficient manner. The early period of Cloud Computing itself gained immense attention and has also attracted enormous users to transform their data centers present locally into cloud servers present remotely.



One of the most critical issues in storing data remotely is data security. On one side, it is necessary to strictly protect sensitive information before allowing the users to use the appropriate data

services. On the other side, users do not have their data physically in remote data storage.

In traditional methods of access control, reference monitors can be completely trusted but remote data servers cannot be trusted by users to implement access control policies. Thus a user enforcing data access control is required for remotely storing the data. Various cryptographic methods allow the user to implement data access policy where the encrypted form of data is stored on the servers which retains the secret key(s) the user control access is established by giving the equivalent data decryption keys. In untrusted storage, Attribute-Based Encryption (ABE) provides the best cryptographic foundation for a securing data sharing schemes.

Cloud computing technology delivers the computing resources through internet. In cloud computing technology, the computing resources are all shared and the clouds are divided into several types based on the locations of the users. The public clouds are either free for usage or paid based on usage. They owned and functioned by the cloud providers. Social networking services, e-mail services, online storage services, etc are all few best examples for public clouds. The cloud infrastructure of private clouds deals entirely for a particular company, and is handled by that company or a third party. Eucalyptus, VMware, Elastra, Microsoft, etc are all few good examples for private clouds.

There are three service models based on cloud computing which are SAAS, PaaS and IaaS. The SaaS denotes the Software as a Service, PaaS denotes the Platform as a Service and IaaS denotes the Infrastructure as a Service.

RSA Algorithm

The RSA algorithm's security relies on the factoring of large numbers being chosen. The RSA algorithm is at present very secure because presently there are no faster techniques for factoring large numbers.

DES Algorithm

DES is a symmetric lump of mystery code actualized by IBM. DES uses a 56-bit key to encode/interpret a 64-bit piece of message. The key at all the times kept as a 64-bit lump, each eighth piece of that is disregarded. Yet, it is regular to put each eighth piece so that each arrangement of 8 bits has an odd no. of bits spots to 1.

3DES Algorithm

In cipher science, 3DES is the natural term for the Triple Data Encryption Algorithm (TDEA) symmetric-key lump cipher texts that utilize the DES cipher text calculation 3 rounds to individual information chunks. The primitive DES cipher text's key size of 56 bits was typically enough when that calculation was created, however the availability of cutting edge advances made brute power helpless against the framework. 3TDES offers a similarly simple method for mounting the key size of DES to safeguard from such vulnerabilities, are defined along with other attributes.

MATERIALS AND METHODS

In this proposed scheme, all the data files are assigned with a list of attributes that are needed for the access control mechanisms. The diverse data files include a set of overlapping attributes. A version number is linked with each of the attributes for the updating of attributes. An attribute history list also called as *AHL* is maintained by the cloud server which is used for recording the version development history of the attributes and the proxy re-encryption keys that are used. One replication attribute

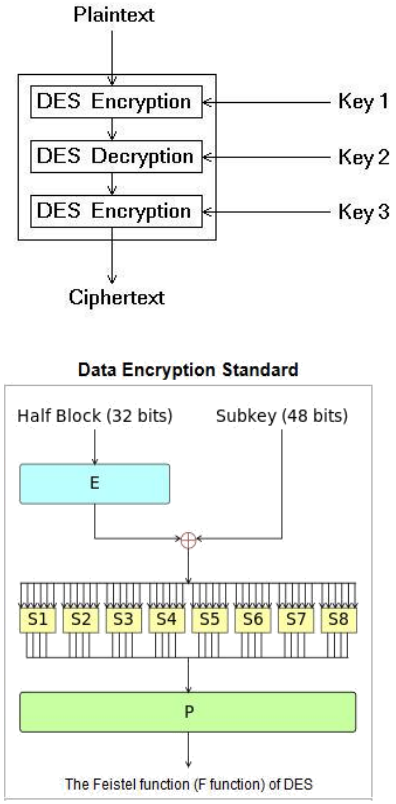


Fig: Architecture of 3DES

This replication attribute is represented by symbol *AD* for computation allocation and key management. *AD* should be inserted inside all the data files containing the set of attributes and it cannot be updated. An access tree is used to implement the access structures of all users. The entrance gates are the interior nodes present in the access tree. The leaf nodes present in the access tree is related to the data file attributes. The root node should be an *AND* gate like *n*-of-*n* entrance gate which has one child node representing a leaf node related to a replication attribute, and another child node related to the entrance gate. This is required for the computation allocation and key management. The replication attribute is not joined to any other node belonging to the access tree. It explains this methodology with an example. The cloud server also maintains a user list *UL* which is capable of recording *ID*s belonging to the valid users present in the system.

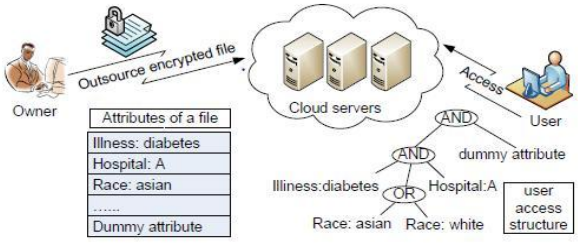


Fig: An Example Case in the Healthcare Scenario
Security Prospect by Multi-cloud Architecture

This model receives many results from one of the operation carried out on a different cloud and compares it inside its own premises. The evidences on the truthfulness of the results been carried out is given to the users. As an alternative to execute an application on only one particular cloud, these operations can be executed on different clouds. Using this technique, the trust on the cloud provider is reduced greatly. Thus as a substitute for completely believing only one cloud provider, it is only necessary for the cloud users to depend on the assumptions, that the cloud service providers does not merge maliciously with it.

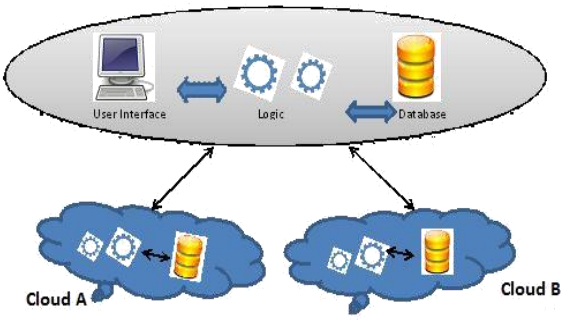


Fig: Replication of Application Systems

Partition of Application System into Tiers

This model separates the logic from the data and provides extra protection on the data leakage because of the application logic. This architecture focuses on the risks on the data leakage that was unnecessary. For reducing the risks of data leakage occurred because of application logic faults, the divisions on the system tiers of the application and the allocation of different clouds are developed which is depicted in Fig. During the failure of applications, the data is not under immediate risk because they are physically divided and safe guarded using an access control model that is independent. It is possible for the cloud users to select a particular trusted cloud provider to store data and diverse cloud providers for the applications.

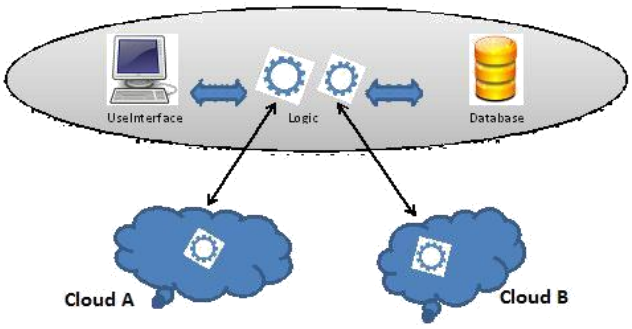


Fig: Partition of Application System into Tiers

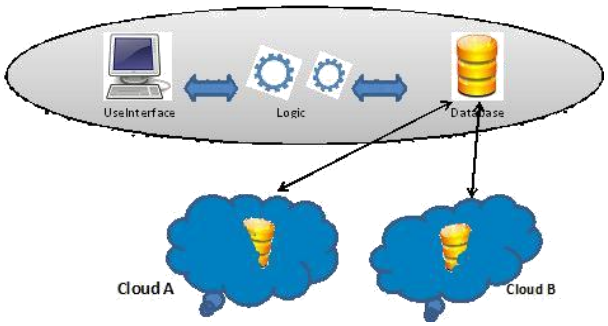


Fig: Partition of application logic into fragments

Databases in general have structured type of data which are in the form of rows and columns. Data partitioning is carried out when the several parts of the databases like rows, tables, rows are distributed to different cloud service providers. Sometimes the files also consist of structured data like XML data. In such cases, those data is partitioned with the same techniques used in databases. The XML data is divided above the XML element level. But this results to be very expensive. For this reason, cryptography based data splitting techniques are followed.

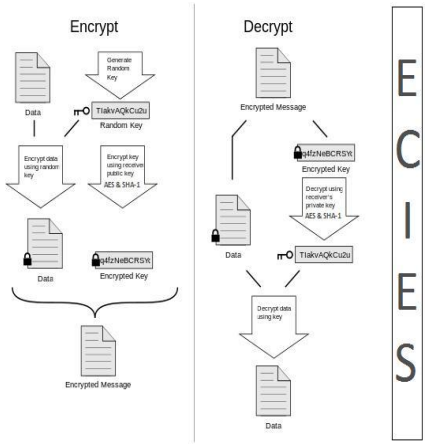


Fig: ECIES (ECC + AES) Encryption and Decryption

ECC Algorithm

Both the efficiency and security features present in the encryption process and the decryption process are handled well in this ECC which is a standard algorithm. Always the ECC algorithm is combined along with other algorithms like DSA, RSA, AES, etc and used together. Based on the researches made, AES algorithm was considered to be the most appropriate algorithm to be used with ECC algorithm and results in a new algorithm called ECIES denoting both the ECC and AES algorithms. This new ECIES algorithm provides more efficiency and more security.

Serialization & De-serialization

The technique to store the data of objects present in the physical memory is known as serialization. An object holding the complete encryption details about the data and constant security certificates is fetched as a result after the process of encryption. When the data is read from the constant files and converted into an object is called as the process of de-serialization.

Serialization

```
FileOutputStream fileOut
 = new FileOutputStream(File_Name);
ObjectOutputStream out
= new ObjectOutputStream(fileOut);
out.writeObject(enc);
```

De-Serialization

```
FileInputStream fileIn
= new FileInputStream(File_Name);
ObjectInputStream in
= new ObjectInputStream(fileIn);
dec = (ECIES) in.readObject();
```

Data Security in Multi-Cloud

The number of data owners denoted by *n*, one proxy server, one TPA and two cloud storage servers and one TPA. The storing and retrieving of the data are enabled by the data owners. Proxy server is used got communication with the cloud storage. To encrypt and decrypt the data using the ECC algorithm, the SHA-1 algorithm is used.

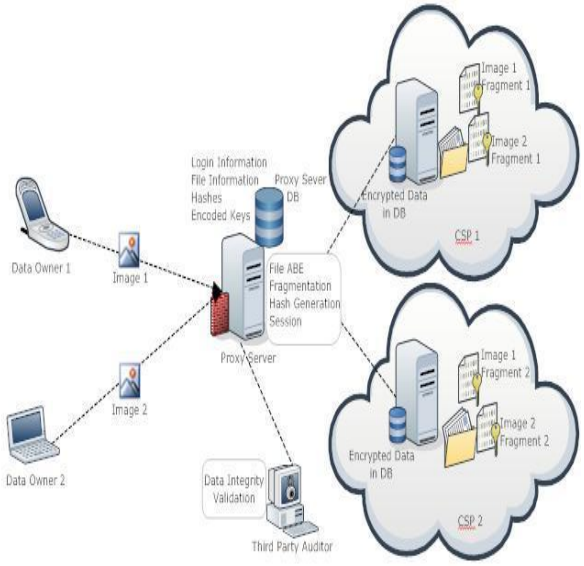


Fig: Data Security in Multi-Cloud

File search in Mobile Cloud Computing

Cloud computing allows the users store their data remotely and also process those data with high speed using faultless transmission. For this reason, cloud technology is used by the web users and also the mobile users. But the only issue to be managed is the security. The files and documents of the mobile users are all stored on the cloud and then later searched using specific keywords in app's search engines. Search engines allow the users to fetch the required information among large piled data present on the server. Several apps make the connection to cloud servers possible, thus allowing the mobile devices to fetch many services. Such apps are utilized for better infrastructure and efficiency. When the data is stored remotely, then confidentiality is a major problem. With fine grained access mechanisms, only the documents meant for the users must be accessed by the users. The pre-computation of Term-Frequency Keyword is needed to search the files present inside the database. The Term-Frequency Keyword related with the equivalent file item is required. This mechanism allows the applications in finding and displaying the right list of files based on the ranks.

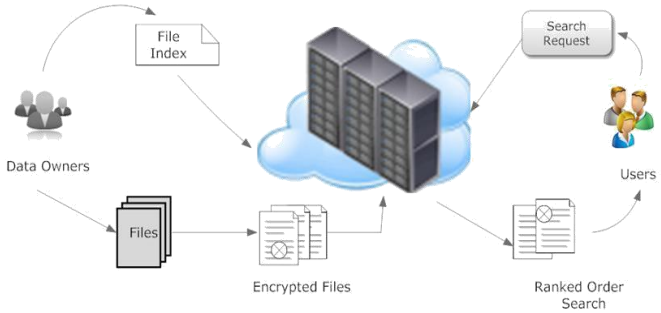


Fig: Encrypted Data Search over Cloud

Mechanism Description

The scheme has seven algorithms: Init, Encrypt, KeyGen, ReKeyGen, ReEnc, ReKey, and Decrypt. The authority performs Init, KeyGen, and ReKeyGen algorithms and the proxy server performs ReEnc and ReKey algorithms. The encryptors and decryptors calls the Encrypt and Decrypt algorithms respectively. ReKeyGen is specified for generating the proxy re-keys. For the re-encryption of the data files, the ReEnc alogorithm is used. The proxy servers use the *ReKey* for updating user secret keys. The version information denoted by *ver* indicates the development of the master key as the following: it is initialized to one initially and it is increased by one when attribute revoking occurrence happens and the master key is then defined again. The public keys, cipher texts, the secret keys and the duplicate re-keys must be joined to the information regarding version denoting the version of the master key.

DISCUSSION

In the proposed architecture we keep information access control in multi-authority based cloud information storage, as outlined. We have five classifications of elements in the plan: Data Owners (DOs), Data Consumer (Group Users), a Certificate Authority (CA), the Attribute Authorities (AAs) and a Centralized Mobile Cloud Server.

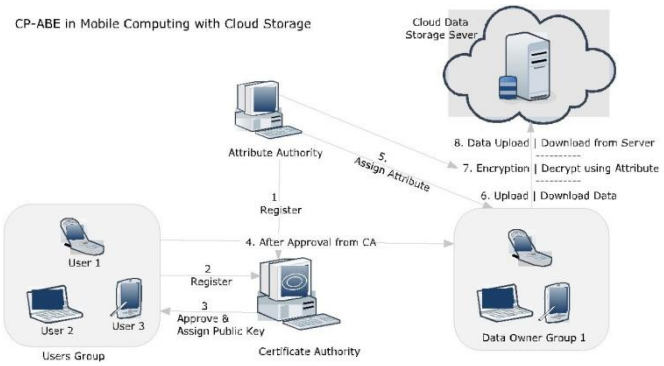


Fig: Architecture Diagram

In this scheme it is consider CA to be a genuine entity that appropriates the approval authentications to the individuals in this association. It provides approval for the new clients and Attribute Authorities. Each genuine client in this plan gets a recognized enrolment ID and a PK (Public Key) is created for them by the CA. In this manner, the certificate authority is not dependable to create or relegate any credit to the clients. Each Attribute Authority is a self-governing entity which deals with creating qualities, relegating it to the clients, disavowing client's access controls and rekeying. In our framework, single trait is connected with an AA, however every AA can direct any measure of characteristics. Every AA has complete control over the course of action and association of its traits; additionally it is at risk to create a secret attribute key for every attribute it produces so that the information can be scrambled utilizing the same secret key according to the

part and gathering of the information owner.

Each client of the framework has a universal enrollment ID, which distinguishes them from each other. One client may be qualified for different properties which are allocated by numerous AAs. Client gets a secret key joined with the properties it claims doled out by a separate AA. A client might login through their gadget and act as an information owner to transfer their content which can accessed by their group. The substance transferred by information owners get scrambled utilizing the secret key they own for their attribute. The entrance strategy gets limited to the information transferred by the owners as it get encoded and stored on the centralized cloud server. Customers of the information must and ought to have the same ascribe keeping in mind the end goal is to decode and get access to the data.

CONCLUSION

Data outsourcing to from mobile devices to cloud servers is not a thing of future. In our everyday life we use many applications which store and retrieve data from remote cloud server to reduce load on resource constraint mobile device also there is a huge advantage come along such as centralization and sharing of data among multiple users. Group level sharing and authentication using ABE are studied vastly by numerous scholars till date but are limited to web users or web applications. There is very little or limited study on group level authorization and authentication of users in mobile cloud computing using CP-ABE mechanism resolving attribute revocation problem. It was tried to propose novel schemes in this regard so that the system model can be made more robust and resilient from unauthorized access.

At last it can be summarized that due to dynamic nature of mobile devices and limitation of resources there is always a need of centralized platform where data can be outsourced and computational overhead can be shared. Web services in mobile computing help to achieve this task but again security is another major concern if data has to be shared within groups. ABE techniques integrated with fine grained access control can solve the security issues but need efficiency in terms of mobile computing. The above discussed proposed architectures can be of much value in maintaining equilibrium of sharing and security of data with performance. Mechanisms are proposed to have an efficient mobile based search on encrypted cloud data, data security with ABE in multi-cloud environment and architecture to solve attribute revocation problem. The solutions proposed are evaluated in real time devices and environment and are proved efficient on various parameters. Symmetric algorithms keeping aside asymmetric algorithms. For extensions to this work asymmetric algorithms may also be studied to find out best efficient encryption mechanism on mobile.

BIBLIOGRAPHY

- M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.Amazon Web Services (AWS), Online at http://aws. amazon.com.
  Google App Engine, Online at http://code.google.com/appengine/.
- Microsoft Azure, http://www.microsoft.com/azure/
- J. Anderson. Computer Security Technology Planning Study. Air Force Electronic Systems Division, Report ESD- TR-73-51, 1972. http://seclab.cs.ucdavis.edu/projects/history/.
- ACL. http://en.wikipedia.org/wiki/Access control list
- H. M. Levy, “Capability-Based Computer Systems”, Digital Equipment Corporation 1984. ISBN 0-932376-22-3.
- NIST. “Role Based Access Control (RBAC) and Role Based Security”. http://csrc.nist.gov/groups/SNS/rbac/
- C. Lynch and F. O. Reilly, “Processor choice for wireless sensor networks,” in REALWSN„05: Workshop on Real-World Wireless Sensor Networks, 2005, pp. 1–5.

- F. Pagano and D. Pagano, "Using In-Memory Encrypted Databases on the Cloud," Proc. First Int‟ l Workshop Securing Services on the Cloud (IWSSC), pp. 30-37, 2011.
- R. H. Deng, J. Weng, S. Liu, and K. Chen. Chosen-Ciphertext Secure Proxy Re-encryption without Pairings. In *Proc. of CANS „08*, Berlin, Heidelberg, 2008.
- S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In *Proc. of VLDB „07*, Vienna, Austria, 2007.
  M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus: Scalable Secure File Sharing on Untrusted Storage. In *Proc. of FAST „03*, Berkeley, California, USA, 2003.