I.J. Computer Network and Information Security, 2014, 10, 48-56
Published Online September 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.10.06

A Smart and Generic Secured Storage Model for Web based Systems

P.Iyappan
Research Scholar, Department of Computer Science & Engineering, Manonmaniam Sundaranar University,
Thirunelveli, Tamil Nadu, India
Email: iyappan@smvec.ac.in

Dr.V.PrasannaVenkatesan
Associate Professor, Department Of Banking Technology, Pondicherry University, Puducherry, India
Email: prasanna_v@yahoo.com

Abstract**—**Nowadays, Recent developments shows that, Cloud computing is a milestone in delivering IT services based on the Internet. Storage as a Service is a type of business model which rents storage space for smaller companies or even for individuals. The vendors are targeting secondary storage by promoting this service which allows a convenient way of managing backups instead of maintaining a large tape library. The key advantage of using Storage service is cost savings of hardware and physical storage spaces. In securing Storage as a Service model, there is a need for a middleware to monitor the data transmission among cloud storage and various clients. The objective of the system aims at developing a smart and integrated dynamic secured storage model which acts as a middleware in supporting all the primary security goals such as confidentiality, data integrity, and accountability. This proposed model will provide secured data dynamics, access controls and auditability. The secured data dynamics is done by Boneh Franklin-Identity Based Cryptography. This model enhances the accounting model in adding indexing policies and provides security in the audit logs through password based cryptography along with AES. This is a generic middleware assisting the basic security features for any cloud environment, so that it can be equipped for any type of system. The main advantage of the proposed system is to reduce the time complexity in encryption and decryption process and also to provide higher degree of security. We also leveraged the implementation of this middleware in a mail server environment with drive option which poses file storage and enables file sharing among the drive users.

Index Terms**—**Cloud Computing, Data Integrity, Auditability, Accountability, Data Storage, Data Dynamics.

I. Introduction

Cloud computing is an IT delivery model [2][14] in which resources are retrieved from the server through internet using web-based tools and applications rather than a direct connection. Data servers are used to store and retrieve the data and software packages. In securing Storage as a Service model, there is a need for a middleware to monitor the data transmission among cloud storage and various clients. Generally Third party verifiers [3][12] are used to manage these services between cloud and client system. Though there are various third parties are available as an individual in managing the transmission of the data, there is a need for an integrated security[1] model to provide secured transaction between cloud and client system. Among those verifiers, the third party accounting system is used to examine and verify the data sharing in the storage to ensure that the unauthorized person do not access the information. One more major third party system is available for auditing and tracking the data modification in the cloud by the clients and it will audit the action done by the client. The goal of our work is to provide integrated secured storage model in which it acts as a generic middleware by supporting basic security goals.

The organization of the paper was represented as follows. The Section 2 contains works related to third party verification and its issues and challenges to overcome. The Section 3 contains proposed system with secured data dynamics for encryption and decryption, Accountability by saving and retrieving the audit logs, and finally with authentication and authorization. Section 4 discusses case study on mail server environment by deploying the generic middleware model and its performance were measured.

II. Related works

Many of the works related to security on cloud environment shows that there was an essential need for the middleware in the cloud environment [5], specifically focused on auditing and accounting system [9][11]. In existing model, it works based on third party auditor. The third party auditor [13][15][16] which tracks the data modification in the cloud by the clients and it also audit the action done by the client. The third party Auditor supports data dynamics by considering the major attributes called manipulation of data through in several ways such as inserting new data, deleting existing one , if needs modification if any are all considered as major step towards practical observation, because cloud computing are not limited to store the data whether in archive or back up process only. Public Auditability can be supported effectively by using public key cryptography based homographic authenticator by exploring BLS and RSA signature scheme[5] which uses a certain pairing function for verification.

Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou also took about auditing and data dynamics. The importance of dependability of data and providing redundant free parity vectors depends on erasure correcting code in the file distribution process. Reed- Solomon technique [4][20] is used to achieve the integration of storage correctness insurance and data error localization. They also provide the extension of the proposed scheme to support third-party auditing by the linear property of the parity vector of Reed-Solomon code. Reed- Solomon Code linear properties modify the data file while storage correctness assurance was maintained through various blocks level dynamic Operations.

Smitha Sunderswaran, Anna C. Squicciarini, Dan Lin[19] shows that verification of data i.e. is in sharing environment needs to ensure the storage that are not accessed by unauthorized persons who having denial of access is done by third party accounting system. In this paper Cloud Information Accountability (CIA)[19] is mainly used for conducting automation of log in the storage and auditing in distributed environment. It consists of two attributes namely logger and harmonizer. The role of logger is to provide automatically logging access to the data when coupled with user's data and also it encrypts the log record using public key. Auditing is done by log harmonizer that generates master key which holds identity encryption through decryption key. It also supports the user access to the log files.

ISSUES AND CHALLENGES IN THE SYSTEM

- In major cloud computing environments, third-party auditing system which uses BLS and RSA for auditing and Merkle Hash Tree authentication[13] for creating data dynamics is not highly securable in distributed environment which is having multiple server for communication of data due to Byzantine failure. It causes hardware failures, deadlock and attacks. Byzantine failures occur during the execution of algorithm in the cloud. It may be one of the following failures. Failure occurs in receiving request, Failure of sending request and response, Incorrect processing of request, local state corruption and sending incorrect response to request.
- The system for ensuring distributed accountability for data sharing in the cloud still need to refine their approach to verify the integrity of the JRE and the authentication of JARs[19]. At the same time they need to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content which will support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls. These indexing policies will organize the accounting scheme and log file. It also helps to manage and retrieve the log files. These indexing policies are lagging in the existing accountability system [10][18]. It should provide software tamper resistance to Java Applications where it should contain measures to prevent a user from modifying it against the data owners or removing a restriction on how it can be accessed because it may lead to malicious insiders, data integrity and other data security issues.

Based on the various related works, we found that there is a need for integrated security model targeting different levels of security of data for a typical cloud infrastructure was necessary. The idea behind the paper is to provide an integrated secured storage model which will poses primary entities of any data security model such as confidentiality, data integrity and accountability. This integrated model will acts as a middleware in supporting data dynamics, access controls and auditability. The main objective of the proposed system is to reduce the time complexity in encryption and decryption process when compared to existing system and also provides higher degree of security.

III. THE PROPOSED SYSTEM MODEL

Our main objective is to provide an integrated model which acts as a middleware in supporting data dynamics, access controls and auditability between the client system and cloud storage.

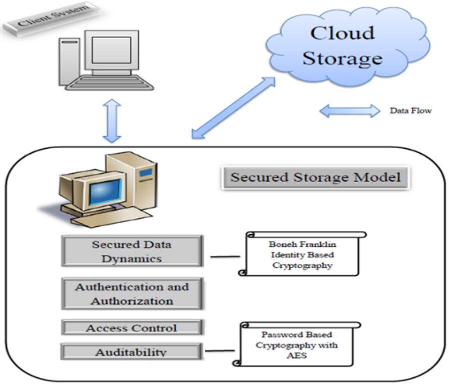

Client System
Cloud Storage
Data Flow
Secured Storage Model
Secured Data Dynamics
Boneh Franklin Identity Based Cryptography
Authentication and Authorization
Access Control
Auditability
Password Based Cryptography with AES

Fig 1: Architecture Diagram

Our proposed model architecture was classified with three different criteria such as Client which has large data file to be stored in the cloud, a Cloud Storage Server, a smart secured storage model and the clients provided with the any client application. The system architecture of our proposed model will resemble as shown in Fig. 1. In order to implement the secured storage model for an organizational based system or any web based systems, it basically requires three basic modules namely a smart secured storage model, a client system and cloud storage.

A. Smart Secured Storage Model

The Smart Secured Storage Model acts as a smart middleware for providing data security which comprises of Authentication and Authorization provided with access control, secured data dynamics and non-repudiated auditing.

Secured Data Dynamics:

It supports data dynamics such as block insertion, modification and deletion, since these services in Cloud Computing are not concerned in archive or backup data. The data sent by the client is received by the middleware and the data is ciphered through Boneh Franklin Identity based Encryption scheme. The ciphered text is transferred to the Cloud storage. When the client system requests data, the ciphered data will be retrieved from cloud after validating the access control. Then the middleware will once again decrypt the data and sent back to the client system. This approach provides data integrity and resilient to modification, replaying and interception. The key exchange can be done through Elliptic curve Diffie-Hellman. The data dynamics are done by as follows:

- User A encrypts the data using User B's email address (userb@company.com) which acts as the public key.
- When User B receives the data, he/she establishes the connection to the key server using the public key.
- After authenticating User B, the key server then transmits his/her secret key, with which User B can decrypt the data. This secret key can be used to decrypt all further data received by User B.

The Boneh–Franklin scheme based identity based encryption works as follows:

(i). **Setup:** Secret Keys are derived from master keys which are kept secret while the parameters used are kept public and used in common. It accepts (a) set of system parameters including the message space and ciphered text space, and (b) a master key.

(ii). **Extract:** This approach is run by the PKG whenever a user requests his/her secret key. It takes parameter, master key and an identifier as input and returns the secret key for user.

(iii). **Encrypt:** It takes the system parameters, a data and outputs the ciphered text.

(iv). **Decrypt:** Accepts ciphered text, system parameters and secret key with User ID returns original text.

The flow of the secured data dynamics for ciphering the data and for getting back the original data is as shown in Fig. 2 and Fig. 3.

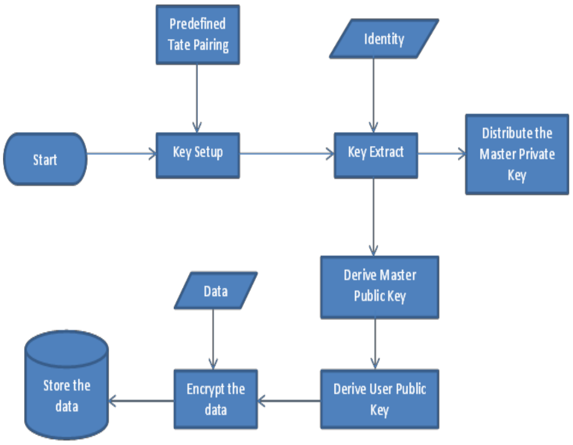
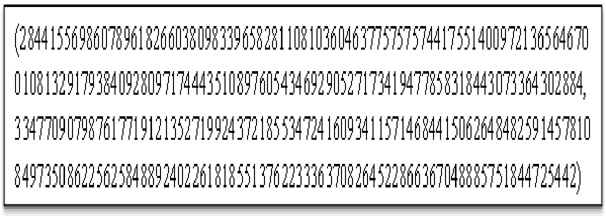


Fig. 2: Secured Data Dynamics for Encryption

After the encryption process, the data will be converted into Field Point as below.



(28441556986078961826603809833965828110810360463775757574417551400972136564670
01081329179384092809717444351089760543469290527173419477858318443073364302884,
33477090798761771912135271992437218553472416093411571468441506264848259145781 0
8497350862256258488924022618185513762233363708264522866367048885751844725442)

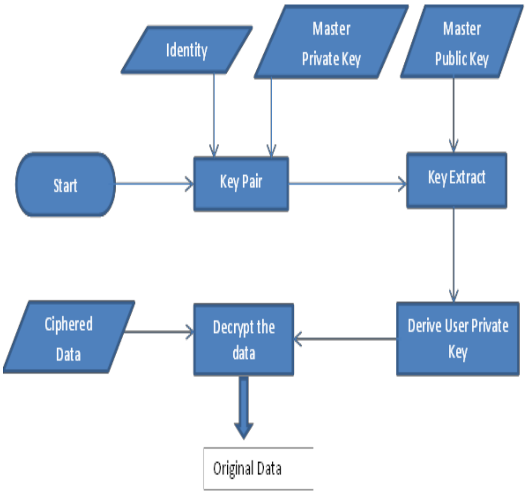


Fig. 3: Secured Data Dynamics for Decryption

The functions of each operation in Boneh Franklin Scheme was used for evaluation.

Accounting the data access:

The auditability component will track the data modification, data access done by the clients in the cloud and it will also audit the action done by the client. It will make a note of each access as a log file to provide data integrity. It will also support a variety of security policies, like indexing policies and generic accountability and provenance controls. These indexing policies will organize the accounting scheme and log file and helps to manage and retrieve the log files. These log files will be in form of XML so that it organized which makes the retrieval process much easier. To secure the files, the AES encryption with password based scheme is used to avoid repudiation. The password along with salt file to provide further security is used to encrypt and decrypt the auditing files. This scheme is done as follows:

- Through the salt file, the system parameter is notarized. With this parameter specification and password, the key is generated.
- With the key, the audit files are encrypted by AES algorithm and stored for every log operation.
- The same password and the salt file are required to generate the secret key (symmetric key) for decrypting the log files by AES algorithm.

The auditing and retrieving the audit logs is schematically shown in Fig.4 and Fig.5.

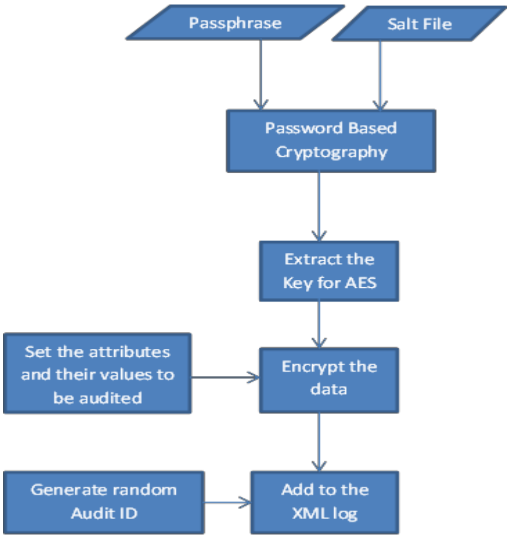


Fig. 4: Saving the auditing Logs

The non-repudiated logs provide data integrity to audited log so that it preserves the proof of each transactions and process done through the clients system on the cloud storage. The following samples shows how the difference in general audit logs organized in the form of XML varied from the logs supported with secured integrity as shown below:

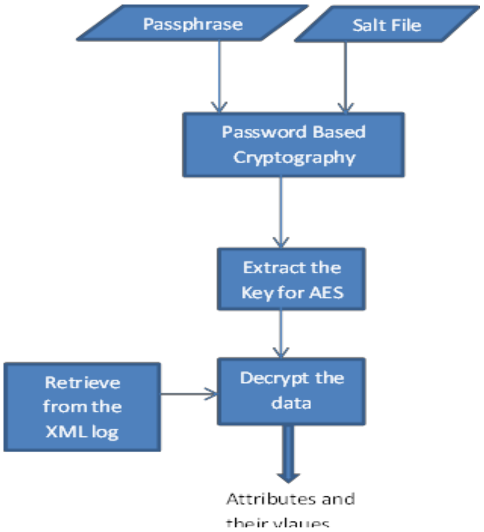

Passphrase
Salt File
Password Based Cryptography
Extract the Key for AES
Retrieve from the XML log
Decrypt the data
Attributes and their vlaues

Fig. 5: Retrieving the auditing Logs

Default Logs:

```
<Audit id="Y01DWEJXcYj">
<AccessedBy> arun91</AccessedBy>
<FileName> Pisa.jpg</FileName>
<FileLocatorID> <lbuEVWdVfje</FileLocatorID>
<AccessMode> Uploaded</AccessMode>
<TimeStamp>Tue, 26 Feb 2013
  20:14:03</TimeStamp>
</Audit>
```

Logs with Integrity:

```
  <Audit id="Y01DWEJXcYj">
  dMTW35UgZrI0oDE3utdtivLfh1ZR65WlNZe2zl4
  eCwVH6/vjfbPRhAzN8rOFIYLsKum8b+VD8Z7P
  KIPDJEhA1fPJaXfItboNplQVixlZV0JKjvR29brO
  uHIEz5hPpP5v1jbw4Aow/NA2OwI8J31yG/iR
  yW1z5a3PDFt86fsaTuGLO/P/3HG7YSgtuNtcSe+
  C63xintL2mIQ2M7DxmWTzWpIvS51gSAAHW3
  EbuUYIDIaCn0E2PwS5U2+9mmkQ1e
</Audit
```

Table 1 – Time Efficiency of RSA Cryptography

Size	Key Extraction Time	Public Key Size	Private Key Size	Encryption Time	Ciphered Text	Decryption Time
IKB	246.666971 ms	419	894	193.838873 ms	1.37KB	37.898468 ms
1.60MB	249.731596 ms	419	894	3037.98088 ms	2.05MB	3997.82379 ms
4.43MB	**215.355093 ms**	**419**	**894**	**6491.140074 ms**	**5.67MB**	**9735.349188 ms**

Table 2 – Time Efficiency of Boneh Franklin Identity Based Encryption

Size	Key Extraction Time	Public Key Size	Private Key Size	Encryption Time	Ciphered Text	Decryption Time
1KB	379.9786 ms	2227	459	106.992896 ms	1.78KB	154.970031ms
1.60MB	353.826049 ms	2227	459	265.464061 ms	1.60MB	387.39021 ms
4.43MB	**382.040701ms**	**2227**	**459**	**404.079917 ms**	**4.43MB**	**711.532688 ms**
10MB	391.696896 ms	2227	459	746.56124 ms	10MB	1437.058594 ms
100MB	438.486307ms	2227	459	4725.429458 ms	100MB	8934.907063 ms

Comparison on Time Complexity:

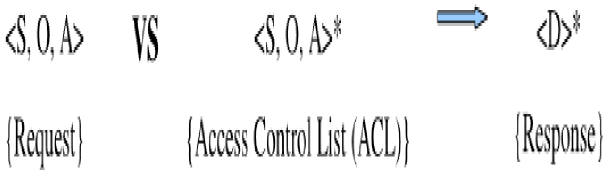
The time efficiency of each operation in the existing scheme and the Boneh Franklin Identity based Encryption schemes are shown in Table 1 and Table 2. For the factors as listed in the table 1 and table 2, we can notice that the time consumed for 4.43MB of data in RSA is higher than the time consumed in ECC - Boneh Franklin Identity Based Encryption. This is because of the reason that RSA uses 1024 bit whereas Boneh Franklin scheme uses only 160 bit for each cycle. This scheme will poses high degree of security as it depends on 3 parameters such as identity, master public key and master private key.

Authentication and Authorization:

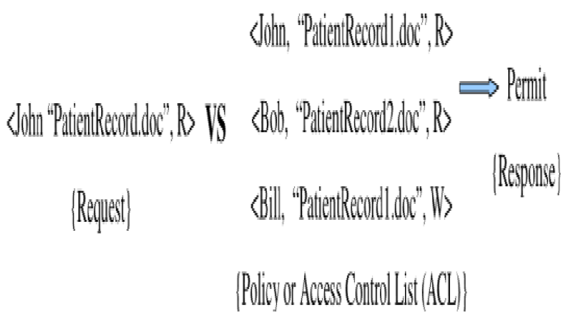
In this, the users of the client system or the client application are authorized with the authorization measures followed by the client system. It provides confidentiality to the storage. The authorization will be done by the Secure Hashing Algorithm (SHA-2). The functional access boundaries will be defined in this section. It follows one-way Challenge-Handshake protocol to support secured authentication and authorization.

Access Control:

The three key rules of any Access Control are: role assignment, role authorization, permission authorization. Consider S as Subject, O as Object, A as Action, D as Decision as shown below.

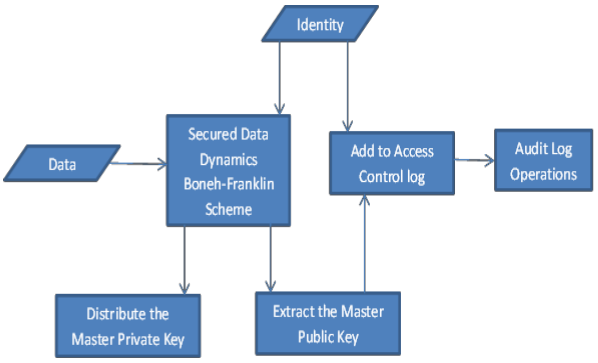


- **Request:** The client system send <S, O, A> as request to the middleware. E.g., <Peter, file, read>
- **Access Control List:** It queues the incoming request as a buffer until decision is made on to the request.
- **Response:** The middleware sends the response <D> after evaluating its policy and then it transfers the control to transaction process.



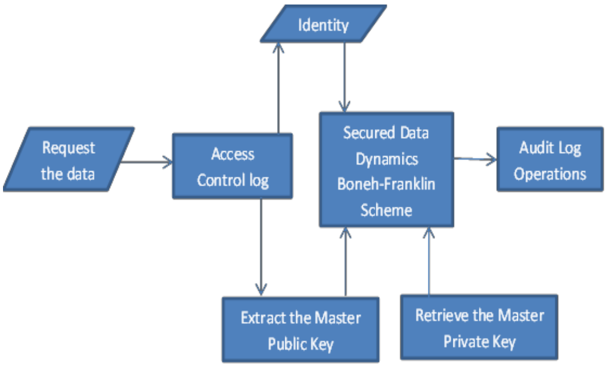
<John, "PatientRecord1.doc", R>
<John "PatientRecord.doc", R>
VS
<Bob, "PatientRecord2.doc", R>
Permit
{Response}
{Request}
<Bill, "PatientRecord1.doc", W>
{Policy or Access Control List (ACL)}

The access control will emulated as XML file so that these parameters can organized easily. The addition and validation of access control is shown in Fig. 6 and Fig.7.



Identity
Data
Secured Data Dynamics Boneh-Franklin Scheme
Add to Access Control log
Audit Log Operations
Distribute the Master Private Key
Extract the Master Public Key

Fig.6: Addition of Access Control



Identity
Request the data
Access Control log
Secured Data Dynamics Boneh-Franklin Scheme
Audit Log Operations
Extract the Master Public Key
Retrieve the Master Private Key

Fig.7: Validation of Access

The sample access control log will resembles as shown below:

```
<Controls>
<Content id="FQJH7NMNAsxzzJT">
<User id="amudhan91">Open, Share, Download,
Delete</User>
<Identity>Hello</Identity>
<MasterPublicKey>
<!--Master Public Key can be stored here -->
          </MasterPublicKey>
          <User id="krish91">Open, Download,
          Delete</User>
          <User id="kavi92">Open, Share,
          Delete</User>
          <User id="arun91">Open, Share</User>
            </Content>
 </Controls>
```

IV. Case Study On Mail Server

This case study aims at developing a mail client that serves the users to send and receive mails and also provides file storage and synchronization service which enables user cloud storage and file sharing. The users can authenticate their identity and then they are permitted to check their mails in their mailbox. Also they can send mails and can delete the unnecessary mails form their mailboxes. They can also organize the files across the folders. This system is processed securely through our secured storage model as a middleware between the mail clients and the cloud storage. The functional requirements for these services are as follows:

Login Page: There will be a login page for the existing user where the username and password are verified and then if he is a valid user, he is allowed for further advancements.

Inbox: The logged in users should be able to see the lists of new mails as well as the existing ones.

Forward option: The user will be able to forward mails from their mailboxes to other mail users.

Compose Mail: User should be able to compose mails and send them to the other users.

Attach files: The user will be able to attach files to the mails and send them to the desired users.

Record Sent mails: There will be a provision for keeping a record of the mails that have been sent by the user in a separate mailbox called Sent mailbox.

Delete: The user will be able to delete mails from their mailboxes.

Organizing the Folders: The user will be able to organize their files among the folders in their drives.

Sharing Folder files: The user will be able to share files from their drives among the drive users.

The mail server architecture with file storage and synchronization service is as shown in Fig. 8.

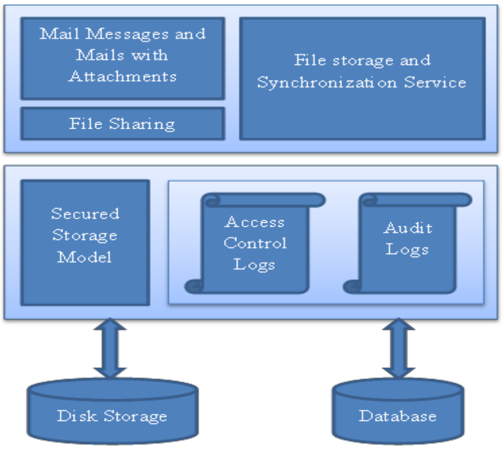


Fig. 8: Architecture of Mail Server

Database Fields Specification:

The format of the table and the required fields used for maintaining the data for this system is described as follows:

Tables:

- **Profile:** This table is used for managing user details.
- **Mailbox:** This table is used for storing the messages and attachment details.
- **Mail Share:** This table will hold the mails that has been shared or forwarded.
- **Drive:** This table will hold details of all the files stored in their drives.
- **Drive Share:** This table will hold the details of the files that has been shared or forwarded.

Table: Profile

Primary Key: userid

Field	Type
userid	varchar(20)
password	tinytext
Firstname	varchar(30)
Lastname	varchar(30)
Dob	date
Gender	varchar(6)

Table: Mailbox

Primary Key: contentid

Field	Type
contentid	varchar(15)
userid	varchar(20)
content	blob
attachments	text
subject	text

Table: MailShare

Field	Type
contentid	varchar(15)
sentto	varchar(15)
dateat	datetime
sentfrom	varchar(15)

Table: Drive

Primary Key: fileid

Field	Type
fileid	varchar(15)
userid	varchar(20)
loc	text
time	datetime

Table: Drive Share

Field	Type
fileid	varchar(15)
sentfrom	varchar(20)
sento	varchar(20)
time	datetime

CLOUD STORAGE:

The cloud storage will have high end processor with robust secured remote access control. The storage can be of structured or unstructured i.e. file system or database. The database server should provide the entire database utilities and other storage measures for the betterment of user data. The storage should highly scalable with taking the consideration of the client system which is going to utilize this cloud storage. It should possess high end network connectivity with the smart secured storage model. The cloud storage is to hold the users' data and all the other information about the client system. The middleware will communicate with cloud storage for users' access and for key distribution.

PERFORMANCE ANALYSIS OF DATA INTEGRITY:

As our main objective is to reduce the time complexity, here we analyzed the time consumption during the encryption and decryption process. The time comparison of the existing scheme and Boneh Franklin based Identity based encryption. The time efficiency of encryption process is as shown in Fig.9.

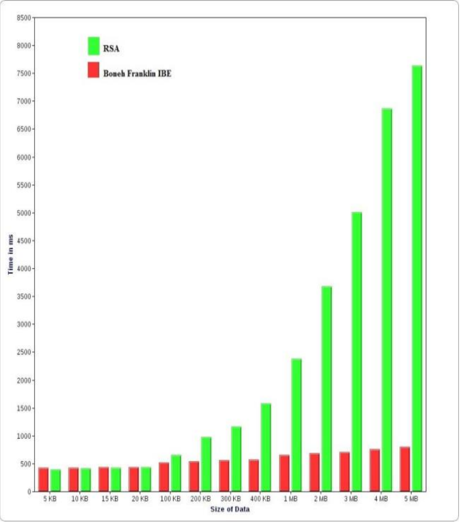


Fig. 9: Time comparison during the Encryption process

The time comparison for the decryption process is as shown in Fig. 10. We can notice that as the data size is increased, the time consumed for both the encryption and decryption for Boneh Franklin Identity based encryption is gradually increased whereas for RSA, there is a steep increase

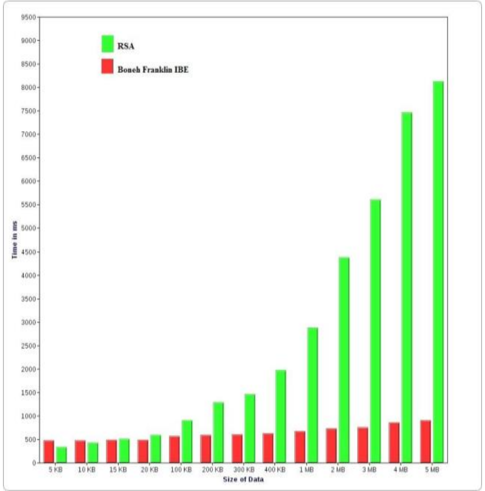
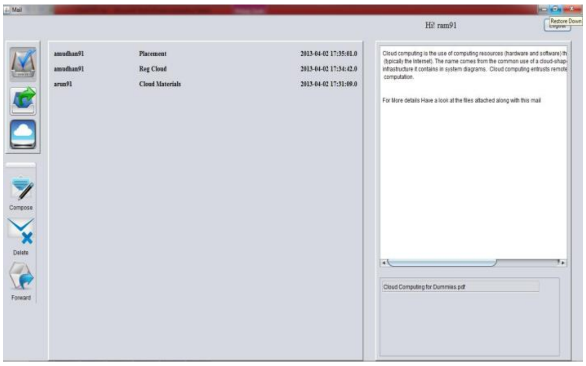


Fig.10: Time comparison during the Decryption process

V. Implementation And Results



Hi! ram91

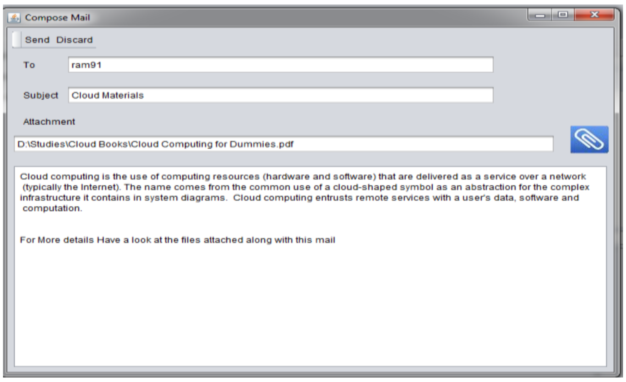
amudhan91 Placement 2013-04-02 17:35:01.0
amudhan91 Reg Cloud 2013-04-02 17:34:42.0
arun91 Cloud Materials 2013-04-02 17:31:09.0

Cloud computing is the use of computing resources (hardware and software) th
(typically the Internet). The name comes from the common use of a cloud-shap
infrastructure it contains in system diagrams. Cloud computing entrusts remote
computation.

For More details Have a look at the files attached along with this mail

Cloud Computing for Dummies.pdf

Fig. 11: Mail Inbox



To: ram91

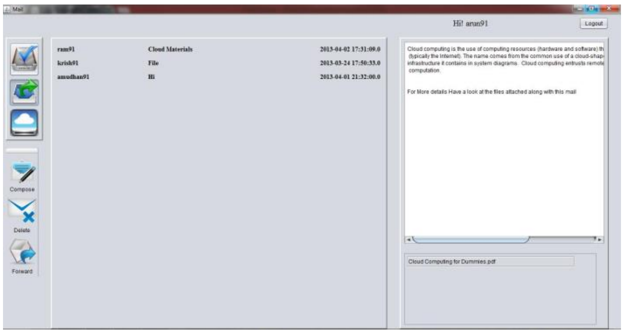
Subject: Cloud Materials

Attachment: D:\Studies\Cloud Books\Cloud Computing for Dummies.pdf

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

For More details Have a look at the files attached along with this mail

Fig. 12: Compose Mail



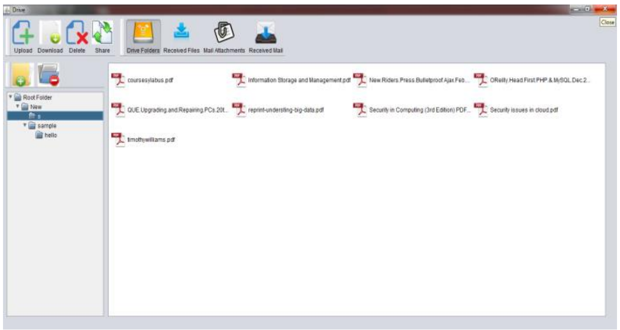
ram91 Cloud Materials 2013-04-02 17:31:09.0
krish91 File 2013-03-24 17:50:33.0
amudhan91 Hi 2013-04-01 21:32:00.0

Cloud computing is the use of computing resources (hardware and software) th (typically the Internet). The name comes from the common use of a cloud-shap infrastructure it contains in system diagrams. Cloud computing entrusts remote computation.

For More details Have a look at the files attached along with this mail

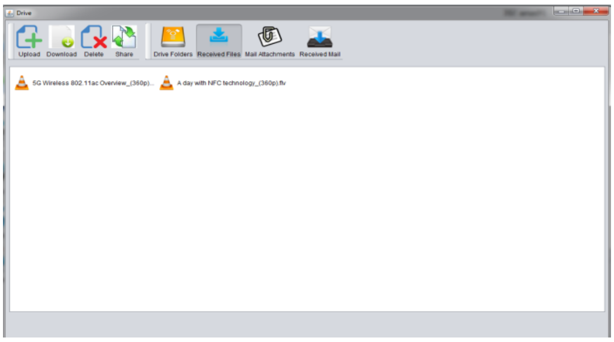
Cloud Computing for Dummies.pdf

Fig. 13: Mail Outbox



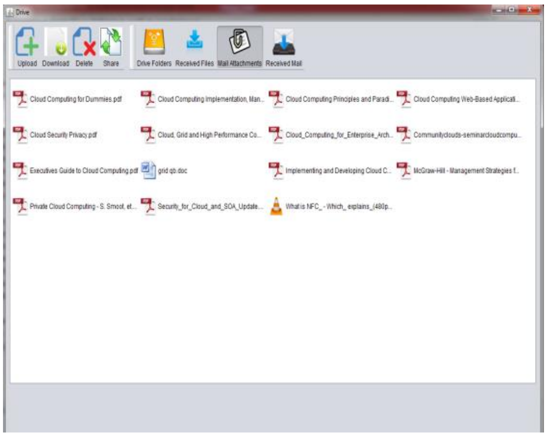
coursesylabus.pdf
Information Storage and Management.pdf
New.Riders.Press.Bulletproof.Ajax.Feb...
OReilly.Head.First.PHP.&.MySQL.Dec.2...
QUE.Upgrading.and.Repairing.PCs.20t...
reprint-understing-big-data.pdf
Security in Computing (3rd Edition) PDF...
Security issues in cloud.pdf
timothywilliams.pdf

Fig 14: Drive Folders



5G Wireless 802.11ac Overview_(360p)...
A day with NFC technology_(360p).flv

Fig. 15: Received Files



Cloud Computing for Dummies.pdf
Cloud Computing Implementation, Man...
Cloud Computing Principles and Paradi...
Cloud Computing Web-Based Applicati...
Cloud Security Privacy.pdf
Cloud, Grid and High Performance Co...
Cloud_Computing_for_Enterprise_Arch...
Communityclouds-seminarcloudcompu...
Executives Guide to Cloud Computing.pdf
grid qb.doc
Implementing and Developing Cloud C...
McGraw-Hill - Management Strategies f...
Private Cloud Computing - S. Smoot, et...
Security_for_Cloud_and_SOA_Update...
What is NFC_ - Which_ explains_(480p...

Fig. 16: Mail Attachments

VI. Conclusion & Future Enhancement

Our proposed model will provide a smart and integrated dynamic secured storage model which assists the basic security for any cloud environment such auditability, data dynamics for storage, access control for Authentication & Authorization. This smart secured storage model is suitable for any cloud environment. This system will provide confidentiality, integrity and accountability which are the primary goals of any security model. The auditability scheme improvises the existing system in providing resilient to data modification attacks as the logs poses data integrity through Password based cryptography along with AES algorithm. This auditability scheme will support a variety of security policies, like indexing policies, security features and provenance controls to organize the accounting scheme and log file and helps to manage and retrieve the log files in much efficient and easier manner which lags in the existing scheme.

The secured data dynamic is done through by Boneh-Franklin Identity based encryption which is much faster than the existing mechanism and it also attains higher degree of security. The use of identity based encryption reduces the complexity in role based or attribute based access control. This integrated secured storage model can be enhanced in the future by providing Service Oriented Architecture which should support the basic characteristics in the realization of SOA in cloud such as Agility, Governance and Multi-tenancy. The system should also be enhanced in supporting interoperability to the middleware so that the system must be capable of correlating with any system irrespective of the platform being used.

REFERENCES

[1] Irshad Ahmad Mir, S.M.K Quadri, "Analysis and Evaluating Security of Component-Based Software Development: A Security Metrics Framework", I. J. Computer Network and Information Security, DOI: 10.5815/ijcnis.2012.11.03, 2012.

[2] Charles Babcock, "Management Strategies for the Cloud Revolution How Cloud Computing Is Transform", Tata McGraw Hill, 2010.

[3] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," International workshop on Quality of Service", July 2009.

[4] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing ", IEEE Transactions on Services Computing, June 2012.

[5] Kumarjit Banerjee, Satyendra Nath Mandal, Sanjoy Kumar Das, "Improved Trial Division Technique for Primality Checking in RSA Algorithm, PP.51-57, DOI: 10.5815/ijcnis.2013.09.07, 2013.

[6] Kuyoro S.O, Ibikunle F & Awodele O, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks, 2011.

[7] Miao Zhou, YiMu, WillySusilo, JunYan, LijuDong, "Privacy enhanced data outsourcing in the cloud", Journal of Network and Computer Applications, February 2012.

[8] Nir Kshetri, "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution", Journal on Telecommunications Policy, 2012.

[9] Pradnyesh Rane, "Securing SaaS Applications: A Cloud Security Perspective for Application Providers," Information Systems Security, 2010.

[10] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, May 2011.

[11] Rajkumar Buyya, James Broberg, Andrzej Goscinski, "Computer Computing Principles and Paradigms", John Wiley & Sons, 2011

[12] Ristenpart T, Tromer E, Shacham H, Savage S, "Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds", CCS, 2009

[13] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", IEEE Communications Surveys and Tutorials, September 2011.

[14] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A and Licciardi A. "Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009.

[15] Smitha Sunderswaran, Anna C. Squicciarini, Dan Lin, "Ensuring Distributed Accountability For Data Sharing In The Cloud", IEEE Transactions on Dependable and Secure Computing, August 2012.

[16] Subashini S, Kavitha V, "A Survey on Security Issues in Service Selivery Models of Cloud Computing", Journal of Network Computer Application, December 2010.

[17] W. Li, L. Ping, X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," International Conference on Electronics and Information Engineering, 2010

[18] Zaigham Mahmood, Richard Hill, "Cloud Computing for Enterprise Architectures", Computer Communications and Networks – Springer", 2011.

BIBLIOGRAPHY

P.Iyappan obtained his B.E in Computer Science & Engineering (2005) from Krishnasamy College of engineering & technology, Anna University. He received his M.Tech in Computer Science and Engineering (2008) from SMVEC, and awarded Gold Medal from Pondicherry University. Currently he is pursuing Ph.D in Department of Computer Science and Engineering, Manonmaniam Sundaranar University. He is having 6 years of teaching experience and one year in software development. His research area includes Service Oriented Architecture, Service Interoperability, Security in interoperation and Web Technologies**.**

Dr. V. Prasanna Venkatesan is currently an Associate Professor, Department of Banking Technology, Pondicherry University. He earned his B.Sc in Physics (1986) from Arignar Anna Arts College, karaikal. He received his M.C.A (1989) from Pondicherry Engineering College, M.Tech in Computer Science & Engineering (1995) from Pondicherry University and Ph.D in Computer Science & Engineering (2008) from Pondicherry University. He is having more than 20 years of teaching experience. He has published 3 books and papers in national and international journals/conferences. His research area includes Software Architecture, Banking Technology, Object Oriented Modeling and Design, Smart Banking. He is co–author of the book titled as Service Composition and Orchestration: Concepts and Approaches published by Vdm Verlag Dr. Muller e.K.

How to cite this paper: P.Iyappan, V.PrasannaVenkatesan,"A Smart and Generic Secured Storage Model for Web based Systems", IJCNIS, vol.6, no.10, pp.48-56, 2014. DOI: 10.5815/ijcnis.2014.10.06