Security for Mobile Application and Its Data Outsourcing in the Cloud Infrastructure

Buchanagandi Enock Nyamajeje, Huiqun Yu

***Abstract*—On the tight constraints in the mobile devices environment, individuals and enterprises are shifting from on-premise solutions to on-demand cloud-based services. More and more application and its data are deposited on the cloud based server for several reasons e.g. scalability, multi-user, ease access, managing expenditure and so on. Cloud infrastructure security issues the risk associated end-user's concern and is also the focus this work's research direction. Therefore, the centralized security solution for insecurity cloud is proposed and the scenarios of this system and methods after that constructed. To solve the problem of data security, by introducing fine-grained access control with this implementation of security-based cryptography protocols. Key authentication and RSA algorithm security service are used by all the end-user for each and every data file access. This security scheme for the cloud is fully fit for restore and effectively safeguard the security of data transmission, data-in-storage and also the storage of the cloud computing. This new kind of centralized security is reliable for cloud infrastructure from solutions that offer data outsourced track to the server running in the cloud and centralized data processing. Also, presented implementation results pilot to the broad applicable, security and allowed end-user has control over her/his data sharing and distribute over the internet.**

***Index Terms*—Authentication encryption, Cloud infrastructure security, Cryptography implementation, Mobile devices, Data Security**

I INTRODUCTION

SMARTPHONES or tablets from Google Android, Apple iOS, Microsoft Window8, Window Mobile, BlackBerry, and Symbian are low-power handheld devices includes running mobile application can be found. Highest penetration of the mobile devices particularly smartphones and the development of mobile broadband are important factors in the development of Mobile applications and services. This increasing is appealing because of wireless technologies are dramatically increasing the network bandwidth capacity. Moreover, these low-powers handheld can also have access appealing to a lot of server resources available to outsource application, and its data are becoming fast and ubiquitous. The mobile manufacturers have opportunistic of reaching toward new services and applications, including social computing, enterprise ads, etc. The expansion of mobile device use has led to the advent of bringing your-own-device trend, a policy that many enterprises and organizations favored. This emerging your-own-device trend has brought biggest issues in mobile application development how to achieve building mobile apps that apply to a handheld. Since, low-powers handheld have differing operating systems, differing screen sizes, and differing attributes. Developing a running program (app) inside mobile devices that runs on many these low-powers handheld provides the cross-platform capability to make the multitude of mobile apps available to both end-users (data user and data owner) [1], [2]. But it creates a lot of tedious task for developers if occurs any implement an application for one set of mobile devices. The firm providing this application must implement additional new devices every few month and has to support all this apps, update and maintain is a lot of effort.

The only alternative solution to the additional new devices problem from these firms and other problems around mobile computing ecosystem is to outsource the application and data to the cloud. Mobile cloud computing is an important aspect and often regarded as a cloud infrastructure enhanced to provide a mobile ecosystem for mobile applications to allow access to business applications from smartphones. Since, the data processing and the data storage happen on the cloud, and the end-users can access the application via browsers. Recently cloud computing has become a mature service model, availability of great scope cloud-computing infrastructure such as Amazon, Google, Microsoft and Yahoo have increased the growth of a large-scale of mobile applications to take advantage of on-demand cloud services[2], [3],[4]. Because of the application and data is being moved from the mobile device to the cloud. The application and data security and privacy are very substantial concerns for the end users. Since there is no longer physically maintain direct control over their data in the cloud server [5], resulting to the implication for security and privacy incentives. These issues pose very significant risks for the end-user concerns are very important top list. Due to high internet speed infrastructure the cloud can connect by just connecting to the internet and the cloud service providers will handle the security and to provides high security to the data. But still based on dominant opinions that is service providers aren't trusted by the end-users, preventing vulnerable application and data need to be kept confidential not only

Manuscript received November 20, 2015; revised December 01, 2015. 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). Security for Mobile Application and Its Data Outsourcing in Cloud Infrastructure.

H. Y. is Dean at East China University of Science and Technology, Department of Computer Science and Engineering, 130 Meilong Road, Shanghai 200237, China. (Corresponding author phone: +86 136 51733116; fax: +86-21-64252984; email: yhq@ecust.edu.cn).

B. E. N. is with the Department of Computer Science and Engineering. East China University of Science and Technology, 130 Meilong Road, Shanghai 200237, China (e-mail: buchana92@yahoo.com).

from other end-users for sharing the cloud services. But also, from the cloud service provider itself, as much as possible. There are many security issue associated with mobile cloud computing and cloud computing. The goal of security researchers is to develop techniques to ensure the application and data security.

In this paper, we proposed centralized security system model comprising based mobile application and its data in the server running in the cloud. This proposed new kind of centralized security for the cloud refers to the mobile devices is being included in cloud security ecosystem. The new challenging security threat points out possible attacks on the cloud-computing inevitably poses that must prevent to ensure secure cloud infrastructure. Moreover, a demand long term continuous assurance the end-user concerns of their application logic and data safety exactly where it stored, whether it replicated and had accessed to it only to legitimate users. The topic of this paper is the adaptation of existing solutions. The underlying task techniques-based are existing proposals, but we have adapted here to a mobile-based cloud infrastructure and environment where data processing, storage happen outside the mobile device. Multiple security applications that check mobile device security can run on the mobile cloud. Despite its need for protection, with SLA guaranteeing the cloud data must remain highly accessible, available for resolving some cloud safety, stability, performance issue, and transitive trust between the cloud service provider and third party cloud. Including the security issues concerns on the cloud server, in this paper we proposed fine-grained access control applicable for prospect to protect unauthorized accessing in cloud infrastructure. Moreover, we provide authentication encryption to secure data files sharing against active adversary sharing user's data file. Other security services including key generation descriptions are provided and discusses in the cloud computing infrastructure system without key-regeneration. While this work did not mention the security issue in mobile environment ecosystem. *We assume that the mobile device is well equipped with security extension of the device's CPU, known as ARM trust zone, providing much broader and more comprehensive security checking for mobile devices.* Some mobile development systems have comparable security features built into their operating systems [6]. Currently, researchers' leverage different structures and techniques in utilizing cloud services/recourses to outsource computation capabilities of mobile devices. The importance of this proposed system is that, the implementation over the lightweight data techniques in mobile cloud computing using encryption methods is to reduce data volume, and I/O tasks. This design and implementation approach may increase a quality of mobile end-user experience. This work contribution is summarizing as follows:

1. The proposed system and methods provide security requirements solution fulfill the following feature for internet service providers and the end-users. Also, the implementation provides security solution for the user and the web services fully integrated security solution (i.e., providing *cryptography authentication, confidentiality, integrity, and nonrepudiation*).
2. The system design and implementation provide secure communication and access control solution that corresponding for the security and privacy to the end user. At the same time, it secures communication between end-users occurring within the cloud infrastructure.
3. The design and implementation based on existing proposals and adapted well-known techniques for resolving some cloud security issues. Here to the cloud computing infrastructure system with the basic background in common security concepts. We figure out what an entity allowed to access with appropriate modification with control security access depending on the roles that end-users have within the system and what access they allow to do assign as appropriate.

The other part of this paper is organized as follows. Section 2 present related work. In section 3, we present the methods and system of centralizing security model for the cloud and formulate the security solution. System design engineering techniques and some detailed analysis are discussed in section 4 and 5 respectively. In section 6, some conclusions and future research are drawn.

II RELATED WORK

A large number of individuals and enterprises are used cloud storage. Because all data store on the remote server where exactly don't have direct control of their data [8]. The only approach remains before outsourcing the mobile app and its data is to encrypt to protect data confidentiality [9]. Data-directed provides to ensure of the system extendibility, scalability, and reliable network connection TCP/IP is generating of the cloud provides powerful management of all the resources [10]. To make full use of information collected by network terminals, TCP/IP used is for communications between the end user's terminals and the cloud server. The emerging of cloud computing has on top of the list [16], [17]. Furthermore, mobile cloud computing has envisioned and pave a way in integrating of emerging cloud computing into a mobile environment ecosystem. Depayan Dev et al.[11] point out the variety of challenges and number of loopholes in the cloud computing ranging from security, limitation of mobile devices, and type of the application that complicate assessing from the cloud computing. Since, the author's work focus on the general overview challenges in the mobile cloud computing. In this paper, we proposed a centralized security system, centralized data processing, safe and transparent data sharing in the system for mobile cloud computing solution for keeping data secure before outsourcing application and its data. We anticipate our work will provide an overview to various concerning challenges related to this field and used as pivot groundbreaker measures to overcome other challenges in the mobile cloud computing infrastructure.

Dijiang Huang et al., [12] proposed innovated system to secure data processing mobile cloud infrastructure. To facilitate secure between the mobile devices and the cloud infrastructure communication in that proposed system, the use of ad-hoc communication system to a blossoming wide solution that provide distributed connective to support a large scale of applications. To this end, our proposed system presents a centralized security, centralized data processing for the cloud infrastructure. Adapt using author's [12] operation of the ad-hoc network in our proposed centralized security system, can enhance communication capabilities and maximized safety and transparent for data sharing and extended cloud's boundary to the end-user domains. While some existing work proposed on ensuring remote data, security lacks the integrity. Q.Wang et al., [13] devote studying enabling public auditing. Author's dedicated to studying the problem and proposed a solution for ensuring integrity of data storage in cloud computing. They consider the task of allowing a third party auditor (TPA) on behalf of the end-users (data owner and data user). Moreover, the solution of using TPA, its purpose mainly is the verification to the integrity of the dynamic data based on the cloud storage. Inspired by their work, in our system security scheme RSA and key authentication based on security cryptography is used for each end-user and every data file access. In our paper, cloud's admin on behalf of end-users does the application assignment to the end-users upon demand. Cloud's admin is a trusted expert provides assistance on behalf of the end-user upon request for any exposed risk of cloud storage services. Moreover, cloud admin does auditing operation to ensure data integrity in the remote server such as viewing user's data graph of various operation activities, monitoring end-user's details, and key management. Pinku.H et al., [14] discuss various potential security loopholes that challenge for mobile cloud scenarios. Authors broadly classified these challenges into three groups i.e. security challenges on cloud services, and communication and mobile application. Comparative to the author's classified mobile cloud security challenges. Our proposed design and the implementation security mechanism have substantial capabilities to overcome most of author's classifies the mobile cloud security challenges. We presented the design and the implementation of the security protocols and innovative that can secure and safeguard the integrity, confidentiality and the privacy of end user's data in the system.

Mykhailo Klymash et al., [15] presented an aware survey on how sharing, retrieval can to optimally utilize cloud-computing services to archive better quality of experience to the end-user. Authors used their modern traffic control mechanisms to generate model simulation processing of traffic. This feature connected with different access technologies such as WiMAX, LTE, etc. allows reliability convergence of the files, video, audio transmission, as well as computing and broadband computing under the single cloud. Comparative with our work, their work scenarios can prove that our centralized mobile cloud security can provide reliable access transmission coverage to the end-users based on underline network topology. Seamless data outsourcing is the crucial requirement in dynamic heterogeneous wireless environments to realize accessing, sharing, and distributed data files. Security and privacy between distributed cloud based server and the end-user are importation requirement in successfully adopting server deployment for an app and its data outsourcing in mobile cloud computing. The security motivation goals are privacy and authenticity of the communicated data. A private-key encryption scheme enables parties in possession of a shared secret key to achieving the goal of data privacy [18].

III METHODS AND PROPOSED DESIGN SYSTEM

Here in this part, we present the design system for the proposed methodology to secure the outsourced app and its data in the server running on the cloud infrastructure. A reliable system where mobile devices are included here in this centralized security of the cloud is proposed. We outline the effective solutions adopted in the mobile based cloud infrastructure. The system under the study is the cloud operating a central remote server that accessed by large mobile users over an un-protected internet network infrastructure. The system connected to the internet via the wireless network through a web browser that with service level guaranteeing. The end users U , $U = (u_i, ...u_{i+1})$ $i = 1, 2, ...n$ can access apps and its data via the browser that runs on a different end-user's mobile devices interface when this app made available on the mobile cloud. To the picture on mind, a highly scalable multi-user mobile based cloud app available to a broader audience. Expectations being toward new services and applications, this highly scalable multi-user cloud system that can be accessed by the multitude of heterogeneous mobile device's users over any TCP/IP network using web services. To this end, TCP/IP suit used for communication, it enabled a large amount of connective end-users domain to communicate broadly globally. To accomplish for the security transparent with based on end-user's demand in means of security challenges protocol such as IPSec is introduced and securing the IP packets. On the other hand, SSL pivot in proving connectivity securely.

A. *System model*

A model/Architecture that depicts key components of the system is as shown in Figure 1. We evidence the end-users in which a mobile cloud hosts the device app and its data. Before to being outsourcing, data files are encrypted before moved to the cloud server; the outsourced data are stored in encryption form and are accessible only after proper authentication. All legitimate end-users can issues data access by registered, and then login to the mobile cloud services and results displayed via browsers running on the end user's mobile devices. The access control server for security assigned to the outsourcing application and its data in the server running in the cloud, enables data sharing and benefits the end-users. In the context of cloud infrastructure problem, the four stakeholders i.e. Cloud storage, Data outsourcing, cloud data, and data user. Considering the four stakeholders and entities can illustrate as follows:

- Cloud storage

Several cloud computing services like Amazon, Google, etc. are ubiquitous, and numerous providers are now exploiting due to their data storage capacity that enables end-users to deploy, move their application and its data instantly to the cloud server.

- Outsourcing

Cloud services considered as a new model of enterprise IT infrastructure, outsourcing sensitive data files to remote server brings privacy concerns. Data storage that keeps the

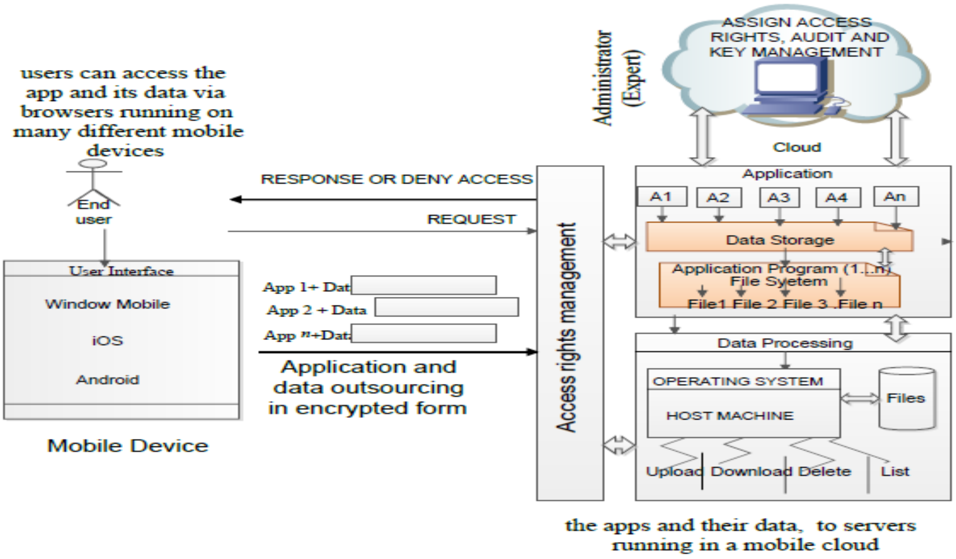
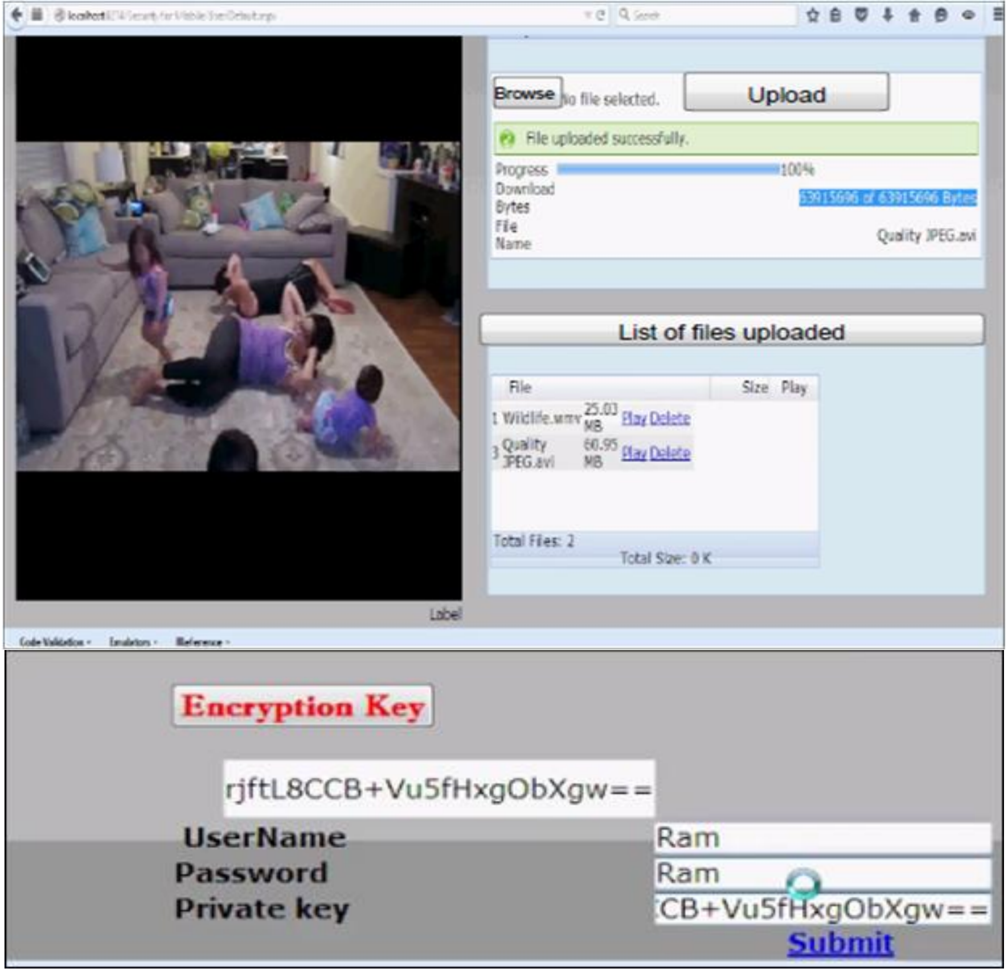

users can access the app and its data via browsers running on many different mobile devices
End user
User Interface
Window Mobile
iOS
Android
Mobile Device
RESPONSE OR DENY ACCESS
REQUEST
App 1+ Dat
App 2 + Data
App n+Dat
Application and data outsourcing in encrypted form
Access rights management
Administrator (Expert)
ASSIGN ACCESS RIGHTS, AUDIT AND KEY MANAGEMENT
Cloud
Application
A1
A2
A3
A4
An
Data Storage
Application Program (1...n)
File System
File1 File 2 File 3 ..File n
Data Processing
OPERATING SYSTEM
HOST MACHINE
Files
Upload
Download
Delete
List
the apps and their data, to servers running in a mobile cloud

Fig.1. Centralized Security Model for the Cloud



File uploaded successfully.

Download Bytes 63915696 of 63915696 Bytes

File Name Quality JPEG.avi

	File	Size	Play
1	Wildlife.wmv	25.03 MB	Play Delete
3	Quality JPEG.avi	60.95 MB	Play Delete

Total Files: 2

Total Size: 0 K

rjftL8CCB+Vu5fHxgObXgw==

UserName Ram

Password Ram

Private key CB+Vu5fHxgObXgw==

Fig. 2. Data file upload.

end user's data may access by cloud service provider or Mitigate theses end-user's data privacy issues, data files should encrypt prior outsourcing to the cloud server.

- Cloud data

We present access control to generate admin authentication key scheme over encrypted cloud data files. This paper proposes secure end user's authenticates from admin over encrypted data files that support dynamic user rank operation on the data file collection.

- Data user

Data users are authorized ones to access the data files of the data owner.

- Cloud server

Cloud server stores the encrypted data collection C for the data owner.

- Cloud's admin

Mediate communication between entities monitors searchable audit log, etc. inside the system.

- Data owner

Data owners are authorized ones to deploy or move their application and its data to the cloud-based server for storage and processing, etc.

A. *Architecture of the system design*

In this paper based on the context of the system and method consists of three different entities i.e. the data users, data owners, cloud's admin, and server running in the cloud. The end users log-in by authenticating into the system. The end-user only involves in basic operations of upload, download, delete, share, search, and view list of data files are the only roles when they interact with the system. The data owners put access label name to their data files and upload to the temporary directory of the system, and then encrypt the data file to ciphertext. After that, the data owners authenticate from cloud's admin and send (submit) data file to the cloud server for storage. Data users can request access to the encrypted data files with their devices to the storage server that require the key. These keys are in encrypted form designed to prevent/ to ensure that untrusted cloud service provider or any malicious attack from learning the information, as means of privacy-preserving. The cloud server alert administrator key management control center when it is safe to do so. Cloud's admin upon data user demand assigns/enforce response access or otherwise and to ensure that availability of data to the legitimate data users as means of access control. After, requests accepted data user authenticate from cloud's admin accompany with auto response key (decryption key) to recover the ciphertext to access the data file.

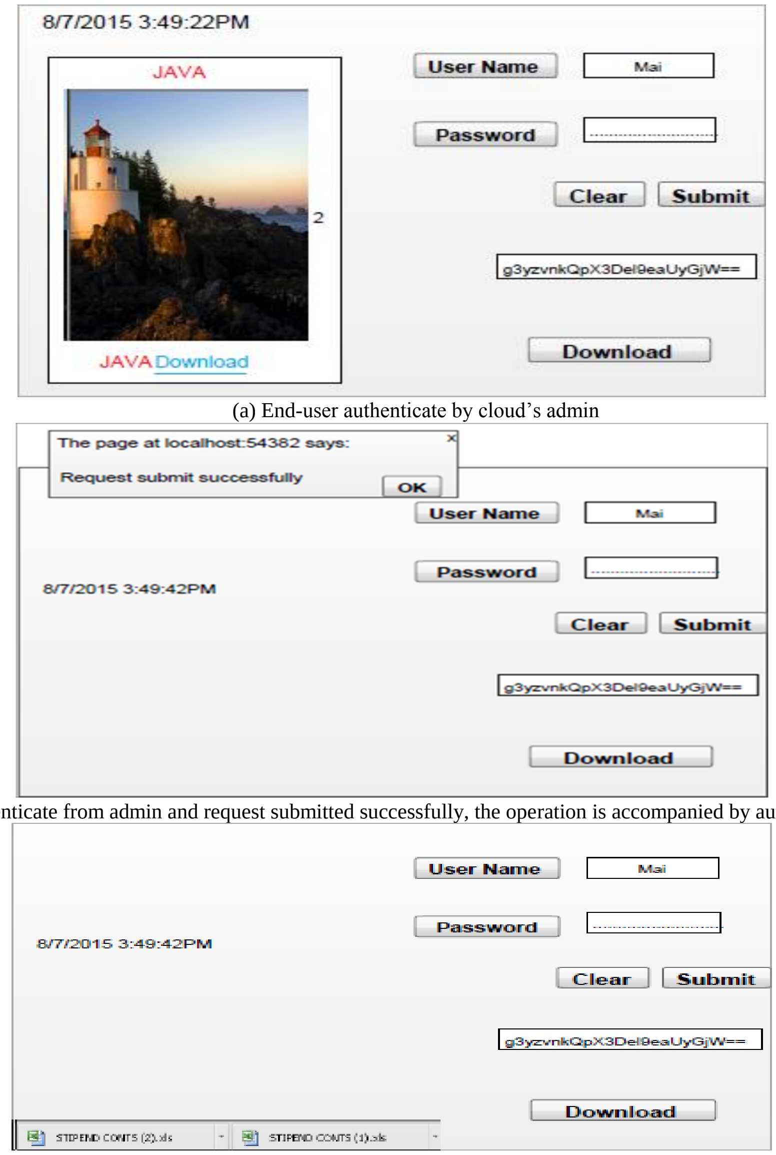
Data mining is not the significant concern, lightweight mobile data considered in this study. Minimizing the overhead to avoid unnecessary energy loss, cost and availability of mobile devices have limited resources such as limited bandwidth/connectivity loss. We propose a centralized security system model that allows the end-users to upload, provide abundant of shared lightweight data file and to ensure security for their data files. To ensure unauthorized access learning users' sensitive information. efficiency distributed of the data file over the internet, the advance search that include "name of school search", "name of the college search", "name of the company search" and friend search (friend name search). An optional of these mechanisms is processing stage that supports multi-keyword ranked search. This advance search and friend search allows the end-user u_i input multiple t query of the keyword of interest to request suitable data files of interest from the hosts. The server then alerts from whomever data owner ($u_i \in U$) the keyword of interest requested belong to and return a response or deny. This mechanism enables data file sharing among different end-users to find (open-source) to search user-friendly based on the friend name search, school name search, college name search, and company name search. This data search existence provided the broad scale of data in one search system. During the protocol execution, the query will trigger the protocol that will allow the end user u_i have access to the corresponding encrypted file m that is from intent user search-list. To optimizing computation expensive and response time for data and data file processing, we target the cryptographic operations protocol in our system design and private key for server optimization performance. The described modules presented in Fig 2, 3, 4, and 5 are experiment snapshots, are illustrate as follows.

Registration and Login Module: Every end-user registered in the individual account in the cloud server. The end users authenticate themselves, the server, checks the username and password and connect to interact with the system. In the system, the end user can have initiate any data operation such as upload, download, share, search, mobile browser, and cloud browser to access data files of interest. End user authenticates from the cloud's admin, and key is required for the end user to access any varies operation varies on the operation requested demand.

Upload Module: The end-users connected and inside the system, the data owner and data user both have the privilege to utilize the system and access data files. The end user (data owner) process start to upload the data files into the temporary directory of the data files binding list in the system. After that, data file successfully uploaded, data owner then encrypt the data file to ciphertext, authenticate by providing user name and password along with cloud's admin accompanied public key. Finally, the end-user submits the encrypted file (data) and sends to the server running on the cloud for storage as ciphertext.

Download Module: Data file downloading, when the end-user want to download data file stored in secure cloud server and since all data files stored in the system are cloud files authentication. The operation prompts the end-user to provide password and user name. After that, end-user can submit the request to the administrative center. When the end-user requests submitted/sent successfully, cloud's admin auto-response accompanied by private key allows the end-user to decrypt data file to recover the data file as plaintext. This access right is also applied on deletion of a data file in the system environment securely and it only occurrences to the data owner. The system provides three options that are “Accept” since other end users have requested for the data file. Another option “Black” if there is data compromising but won’t occur since the system is highly secured. The final option is “Active” to activate the data file for security purpose and to share content, document files, data with friends and families in the system. Moreover, “Delete” option itself which has the same procedure operation with as download.

Share, Search Module: Development of mobile broadband, dramatically increase the bandwidth capacity for the 3G/4G/5G and access to other high bandwidth networks like Wi-Fi through a secure connection IPSec. It is a reason of seamless connectivity communication capabilities to support communication to utilize cloud infrastructure services. Sharing cloud’s data file boundary is extending to end user’s device domains. Since the data stored in the server running in the cloud in encrypted form in secure storage. Key authentication, RSA algorithm is used by all the end-user for each and to every data files access. The cloud server directory system includes a large scale of data files interested in exchanging data files of interest. Each end-user node hosts a multiple of the document, data, audio files that may shared to each other in the system upon corresponding end-user demand. A registry server maintains a directory of all hosts in the system located in the cloud. When the system is querying for services, it returns a subset of hosts, which directly contacted for the services of interest. The procedure repeatedly until the search is successful concluded. Since the end-users are queries selected at random by the system tracking server, this hosts may not always have the desired data files. Therefore, repeated rounds of a query may need to initiate the detection to occur. In query serving operation the end-user coming through making the search request, a server is going to take all end user’s query indexed it. The secure cloud’s admin server is going to find it i.e. the end-user query in the index tables allocated within the system server that data files are the interesting one. In all of these scenarios, the end-user may have multiple index services and multiple data file service. The secure server is going to split out each of these indexes and choose what allows in order applying to the end user.


8/7/2015 3:49:22PM

User Name: Mai

g3yzvnkQpX3Del9eaUyGjW==

(a) End-user authenticate by cloud’s admin

The page at localhost:54382 says:

Request submit successfully

8/7/2015 3:49:42PM

User Name: Mai

g3yzvnkQpX3Del9eaUyGjW==

(b)After end-user authenticate from admin and request submitted successfully, the operation is accompanied by auto-response security key

8/7/2015 3:49:42PM

User Name: Mai

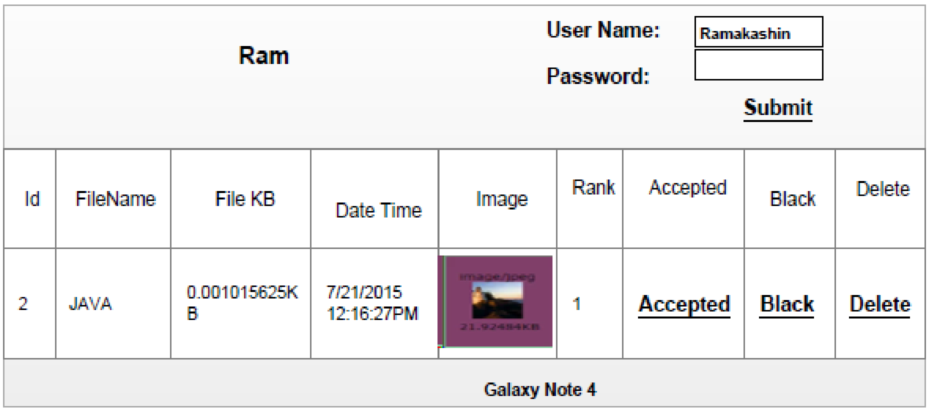
g3yzvnkQpX3Del9eaUyGjW==

STIPEND CONTS (2).xls

STIPEND CONTS (1).xls

(c) End-User led to download and recovered the file

Fig. 3. Data file download



Ram

User Name: Ramakashin

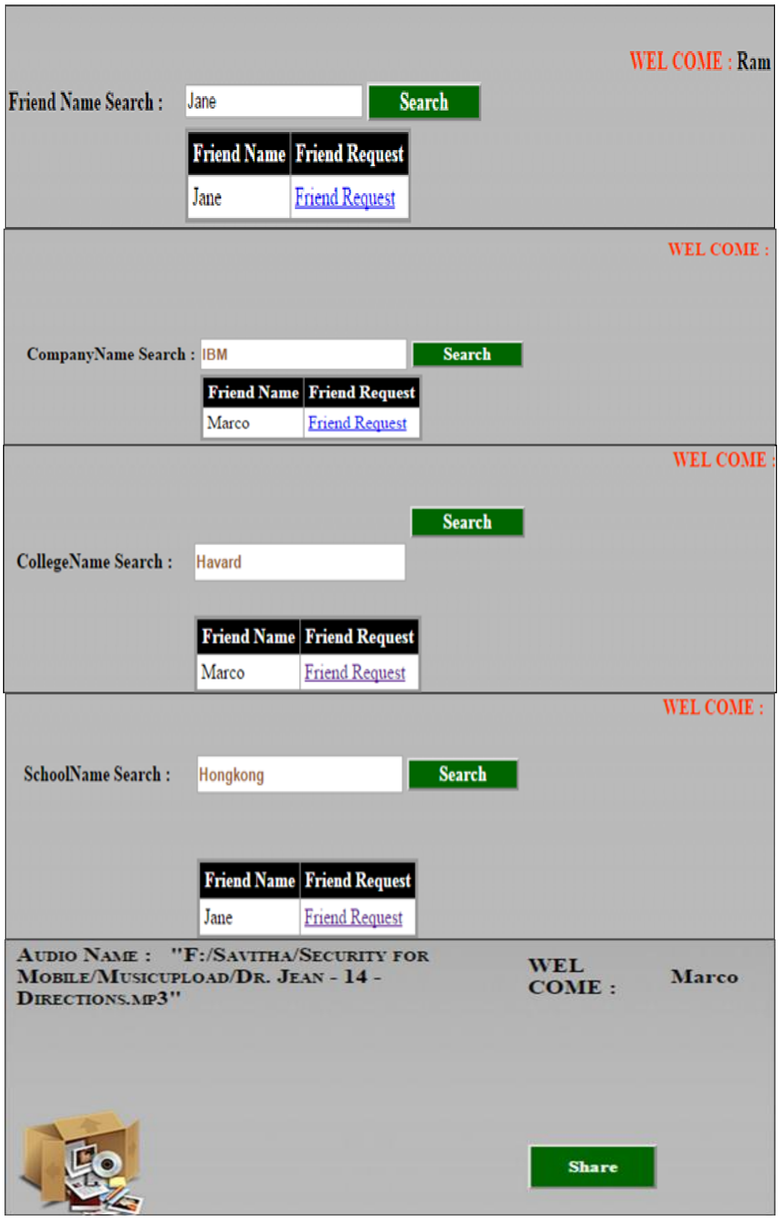
Password:

Submit

Id	FileName	File KB	Date Time	Image	Rank	Accepted	Black	Delete
2	JAVA	0.001015625KB	7/21/2015 12:16:27PM	image/jpeg 21.92484KB	1	Accepted	Black	Delete

Galaxy Note 4

Fig. 4. Data file delete



WEL COME : Ram

Friend Name Search : Jane

Friend Name	Friend Request
Jane	Friend Request

WEL COME :

CompanyName Search : IBM

Friend Name	Friend Request
Marco	Friend Request

WEL COME :

CollegeName Search : Havard

Friend Name	Friend Request
Marco	Friend Request

WEL COME :

SchoolName Search : Hongkong

Friend Name	Friend Request
Jane	Friend Request

AUDIO NAME : "F:/SAVITHA/SECURITY FOR MOBILE/MUSICUPLOAD/DR. JEAN - 14 - DIRECTIONS.MP3"

WEL COME : Marco

Fig. 5. Data files search and data files share

A. Adversary Model

Adversary Threat: The existences of four stakeholders in the context of this paper lead to a creation of different three conceptual network entities i.e. the end-user, cloud's admin, cloud-based server. The use of the mobile could it is important to consider for provision of a unique security. That's possible because the system allows devices to be part of the security scheme of the cloud (i.e. centralized security for the cloud). Outsourced encrypted data files m need the requirement assurance of the existence of sufficiently robust, security and privacy's standard features in the cloud against insider adversaries. Before data/files outsourcing or after its task to the cloud server comes into play to protect from falling into malicious hands and cannot place at risk. That adds core value to the data owner and data user to further protect their proprietary information. We identify and explore security issues, some the common and primary concern to mobile cloud security threats. Some of the security threats scenarios have identified in existing works, such as 1) Browser exploits; 2) Information disclosure; 3) Session Hijacking. Moreover, end user gets an unauthorized access to the management interface is vulnerable for outsiders. The self-service on demand is a characteristic that is essential aspects needs security assessment for the cloud management interface that is accessible to cloud service users, and Internet security protocol vulnerabilities that are the cloud standards requirements in the ubiquitous network access domain should not be exposed via network exploitation customary related of case in standards protocols.

Security model: Secure against eavesdropping and tampering, we ensured both integrity and confidentiality. We recall the definition of authentication encryption (AE) for E, D where usually encryption algorithm takes a key E_k as the message m , absolute nonce N and produces a ciphertext c .As usual:

$$E : E_k \times m \times N \rightarrow c \text{ But: } D : D_K \times m \times N \rightarrow m,$$

$$U\{\perp\}, \begin{matrix} N \rightarrow c \\ \perp \in m \end{matrix}$$

Theorem: let E, D be the cipher that provide authentication encryption (AE). Then E, D is a chosen ciphetext attack secure. An attacker cannot create new ciphertext that decrypt properly.

In the secure cipher let, recall Shannon 1949. Definition: given two messages m_0 and m_1 , using Caesar cipher (E, D) operate over entire (E_K, m, c) have the perfect operations that eliminate fake signed message. Therefore has the perfect secrecy only if $\forall m_0$, $m_1 \in m$ ($len(m_0) = len(m_1)$) and $\forall_c \in c$, $\Pr[E(E_k, m_0) = c] = \Pr[E(E_k, m_1) = c]$ proves that $K \xleftarrow{R} k$. The powerful adversary learns nothing about the plaintext from the ciphertext. Symmetric or asymmetric cipher procedures provide temper resistance and secure storage.

Additionally, verifying the authenticity of the data possession in a remote storage server running in the untrusted cloud is consider to be crucial in realizing safe computing in the cloud infrastructure. The third party stores a file this is designed to provide probabilistic proof to secure them, and using the queried blocks (each block of a file), the server generates a proof of possession. The key authentication serves every end user authenticate from cloud's admin for proof. We implemented Ron-Rivvest, Adi-Shamir, and Len-Adleman (RSA) algorithm [7], building block cipher (RSA) takes every message m which is a mapped to an integer e . In this paper system, the public key is made publicly available and is used only once. Uses matched public/private key pairs the data owner can encrypt with public key data file into ciphertext depending with the sensitivity of the data files, once is stored on the cloud server. Only (one) each end user can decrypt with the decryption (private key) to recover the data file. In Hash function, hash has to be protected in fact that any unauthorized user can alter the data and calculate a new hash value.

B. Design Goals

The goals of our system design based on our methods can summarize as the follows:

1. Have a secure cloud computing infrastructure before end users outsourcing mobile application and its data to the server running in the cloud.
2. Provide centralized security for the cloud and secure centralized data processing to offer safe, reliable, and transparent data storage access and computing to the end-users.
3. Have centralized data, all data shared across, and the end users can access to the most current data files available to everyone inside the system to only legitimate end-users.

IV KEY MANAGEMENT AND ENCRYPTION ENGINEERING TECHNIQUES DESCRIPTION

The focus of this paper is to identify, explore security-based issues on the cloud computing to improve the system by examining the assets, vulnerabilities, entry points, and actors in a cloud. This paper adapts, design, implement, and analyzes the security of a system in a systematic manner (i.e., engineering techniques) to an extent high-level security in the system that malicious user may utilize. Cloud attack surface in cloud computing systems can be i.e. attack on end users to communicate with the cloud over insecure public network and attack on the sharing the infrastructure among multiple end users. Our emphasis will be on multiuser-user services application and its data in the server running in the cloud and interacting with large populations of active mobile devices end-users. We present two different key management models with new innovation design procedure regarding the choices i.e. short-term session keys and long terms keys. The background approach toward security are explored, based on existing proposals and adapted well-known techniques for resolving some cloud security issues to the cloud server with basic background in common security concepts. We figure out which an entity allows to access with an access control depending on the roles that users have within the system and what access are allowed to do assigned as appropriate. The proposed scheme, encryption keys are stored and the keys managed by central administrator center. The fundamental qualities and derived assumption cloud service providers being that it is not trusted. Analyzing of this scheme will help in examining appropriation for defenses against particularly attackers to improve security methods for the RSA in practice. Each node represents entities in the network have and use a matched public/private encryption key pairs. The public key provides part along with the identity of the corresponding ones is stored in a secure central key management repository.

A. *Apply Centralize Key Management Module*

This model, cloud's admin manages administrative center for a key store. Cloud's admin mediates a communication and control access for the end-users that require the key that legitimate can specify and who can connect to the system. Cloud's admin authenticates to gain access to the cloud services using an authentication method in cloud space, which also manages an access control server and key management.

Key Generation: To provide part of required secure to obtain a private (secret) key, public key and cloud file authentication every end-user has to register in the system located in the cloud. Provided a key generator of given a positive integer N of two whole numbers p and q , a group G , G_1 is of a prime number q if there is a given element $g \in G$ such that a generator of G a is given element g which represent the public key generator, computable non-degenerate the map a positive integer $e(g,g) \neq 1$ bilinear pairing the map $e: G \times G \to G_1$ and hash functions such that the security is a random oracle (H, H_1), then be defined by $H(x) = H_1(x)$. Note in typical usage there is free random key choice of both inputs. Useful presenting a bilinear pairing over elliptic curves groups use mathematical trickery, such that:

$\mathrm{H}:\{0,1\}^* \to G$, $H_1 : G_1 \to 0,1^l$ where an ι -bit is the keys length of the plaintext.

Viewed as a collection for all $P,Q \in G$ and $\square_N$ $a,b \in \square_N$ corresponding which is represented the map properties $e(aP,bQ) = e(P,Q)^{ab}$ be able to decrypt the result in polynomial included $\square_N = \{0,1,.....,N-1\}$; $(\square_N)^* =$ {invertible elements in $\square_N$ }. Facts: $e \in Z_N{}^* \Leftrightarrow \gcd(e,N) = 1$ number of elements in $(Z_N)^*$ is $\varphi(N) = (p-1)(q-1) = N - p - q + 1$.

Euler's theorem: $\forall e \in (Z_N)^* : e^{\varphi(N)} = 1$.

The probability is over the random choice. The centralized key administrative center chooses a random secret key, managed by the cloud's admin and always kept secret, it can only be applied to two ciphertexts in two group G , G_1 and the output has G_1 , the decrypt of ciphertext computation of this two group G , G_1 is similarly .

Encryption Module: The data files usually encrypted before moving to the server running on the cloud. In the set-up phase user $u_i \in U$ requests a public secrete key pk and key parameter from key central management center. User u_i chooses a random number $r \in Z_N^*$ in encryption form when selected. For data file m , calculation processing

$$c = E(pk,m) + 2r + pq$$

E : Often randomized

Then produce the corresponding message the ciphertexts. The encrypted message m can then uploaded successfully and stored to the server running on the cloud in a secured form.

Decryption Module: The end user u_i authenticate from cloud's admin sends a download request to the admin or downloads the encrypted data file from the server and sends the decryption request to the admin. The private key accompanies the decryption request sk from central administrative center. This key session setup phase activity must be done only once for each data files to which end user u_i may have access to the data file. The end-user u_i then download the file from the data -list in the server running on the cloud and will be a successful decrypted using private key. Consistence correct purpose for every plaintext (message m)

$$m = (D(sk,c) \bmod p) \bmod 2$$

Since $p \times q < 2r + m$, then

$$(2r+m) \bmod 2 = m$$

D: is always deterministic

B. *Apply Multi-key Level Management Module*

To reduce the authentication traffic load in the server running on the cloud, key authentication has authority to each end-user access to a different data file including access control, integrity, and non-reputation. The entire encryption of data files in the server represented so that the end-users can decrypt on the data file they authorized to access using the private keys without regenerate a key. This operation of key management used for the purpose of confidentiality (encryption) to establish session keys and protect stored data. Access control cloud based server managed by administrative management center handles for authenticates the end users to connect to the system. Also, admin assigns the end-users with access rights share and query friends search request for data files sharing in the cloud space.

Key Generation model**:** At a session setup scheme, cloud-based server managed by cloud's admin run the key generation is randomized that return probabilistic key generation (pk, sk) algorithm, the member of this set are parameterized by security parameter k for each input value and an identifier either a user $u_i \in U$ or adversary. Outputs a corresponding private key sk_i and uses returned matching public and secret keys a pair (pk, sk). This algorithm can be either probabilistic or deterministic. The cloud's central administrative center constructs polynomial in the security parameter $A(x)$ such as that: x is substitute with hash function cryptography $h(x, y)$ from valid end-user possessing a secret key in a group G is 0, otherwise. A polynomial is that evaluate to a random r mapping hash results and useless value. Calculation

Assumes $\mathrm{H}:\{0,1\}^* \to G$ That is, for each value of the security parameter k there is to be a hash function such that is a random oracle.

$$A(x) = \prod_{u_i \in U} \left(x - h(sk, r) \right)$$

$$A(x)_{u_i \in U} \left[A(x), h \right] = \Pr\left[x - h(sk, r) \right]$$ Where

$$sk_i \xleftarrow{R} sk$$

Encryption Module: end-user u_i access the single data file in the cloud. The end-user u_i finds that access to single data file is governed by the random access value r, the end user generates the single data file access key by computing the hash of own private secret key, used for encrypting the original data file encrypts with each users' only the authorized ones who have access to the data file. $u_i \in U$ Encrypts message m as ciphertext using the symmetric single data file access key. End user $u_i \in U$ then authenticate with the cloud's admin to store ciphertext in a single shared data file.

The end-user u_i over (sk, m, c, r) a pair of computing the hash using secrete key and public polynomial

$$sk = poly_{u_i \in U}(h(sk, r))$$

The end user u_i encrypt data file as ciphertext using public key pk , then authenticate with the cloud's admin to upload data file and stores the data file in the server running in the cloud.

$$c \leftarrow E(pk, sk, m) + 2r + pq$$

Decryption Module: Private Key sk_i kept secret by the end user. End user u_i has private key to download data file, request permission to access data file by issuing the key. End user u_i authenticate by the admin accompanied by the private key to decrypt the data file to recover the plaintext and then download the data file.

$$m \leftarrow D(sk_i, pk, c) + 2r + pq$$

V EVALUATION

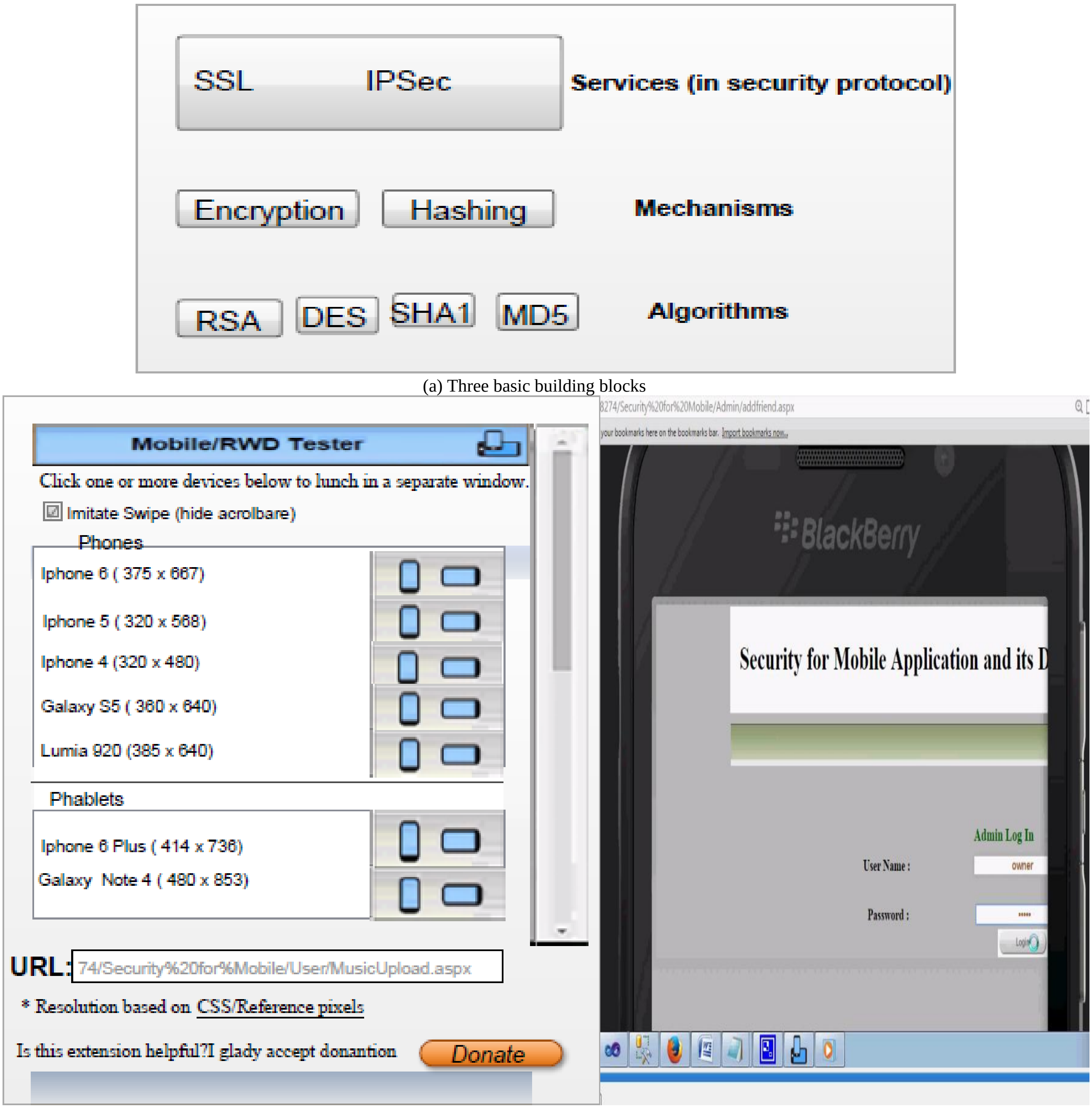
A. Implementation

To evaluate the implementation of the system design, we implemented the system model in front-end visual studio 2010 professional using ASP.Net framework 4 with C# chosen as the language, Operating system Windows 7 Ultimate and Galaxy Note 4 Android used. Also, a cloud emulator web application instance that serves as the cloud in our implementation used to communicate with the application programming interface. The operation needed by the end user implemented as the client application connects with frontend Microsoft SQL Server 2008 R2 to access the services as shown in Figure 6. The communication between stakeholders and entities in the system is secure established and implemented using best.Net packages of security libraries schemes and protocols. All the cryptography operations implemented and used properly using authentication encryption and RSA algorithms on all the base of abstract classes. Most of our experimental graph/chat results obtained with the following hardware specification. The hardware specification characteristics for the server and the end users used are 2.4 GHz CPU, 40 GB, 1.44 Mb Floppy Drive, 14' Color Monitor, Optical Mouse, 512 Mb Ram. The byte coding offers cryptography security services based on the ASP.NET C# framework and enhanced by cryptography protocols.

In this paper as shown in Figure 6 (b) present how the system design implementation using a typical protocol, mechanisms, and algorithms to provide a security service in the system located in the cloud.

B. Implementation Results

Data Files Access Demand: Here we implement the graph of a different kind of data file size of rank quality demand operation based on our experiment results. The experiment results present the access of data files by the end-users in the system (cloud space). Figure 7 shows data file rank, such that y-axis is a rank number of data files requested and accessed in the data file list collection C . While for the x-axis is the name file of the data/files in the ranking results-list. We grouped the data file's graph in three different categories i.e., unique-files rank, data files rank and music files rank. As shown in figure 7 (a) presents end user's each single data file access by selecting of single data file from a comb-box (i.e., right-hand side comp-box present document/files and the left comb-box presents the content files i.e., like music and video). Figure 7 (b) present all end user's different data file access in the system. The dynamic change of utilization of this data file can provide simultaneous assurance of different data file quality of demand with data network access and data retrieval to enable efficient services forecasting exists for its network resource usage. Also, selected features (hosts) may exhibit extensive delay from querying search request. This is due to the distance in the topology of the dynamic network transportation, which in turn would make the exchange of information between the end-user and the network assets (searching) applied to be quite inefficient presenting, in turn lead to costly. This was until then, in [15] authors provide design and implemented (IMS) architecture service innovation. Their modern traffic control if integrated with our proposed centralized security for the cloud will realize elastic real-time communication, especial for data files shared by a large number of the end-users domain.



(a) Three basic building blocks

Mobile/RWD Tester

Click one or more devices below to lunch in a separate window.

☑ Imitate Swipe (hide acrolbare)

Phones

Iphone 6 (375 x 667)	
Iphone 5 (320 x 568)	
Iphone 4 (320 x 480)	
Galaxy S5 (360 x 640)	
Lumia 920 (385 x 640)	

Phablets

Iphone 6 Plus (414 x 736)	
Galaxy Note 4 (480 x 853)	

URL: 74/Security%20for%Mobile/User/MusicUpload.aspx

* Resolution based on CSS/Reference pixels

Is this extension helpful?I glady accept donantion

Donate
8274/Security%20for%20Mobile/Admin/addfriend.aspx
your bookmarks here on the bookmarks bar. Import bookmarks now...
BlackBerry

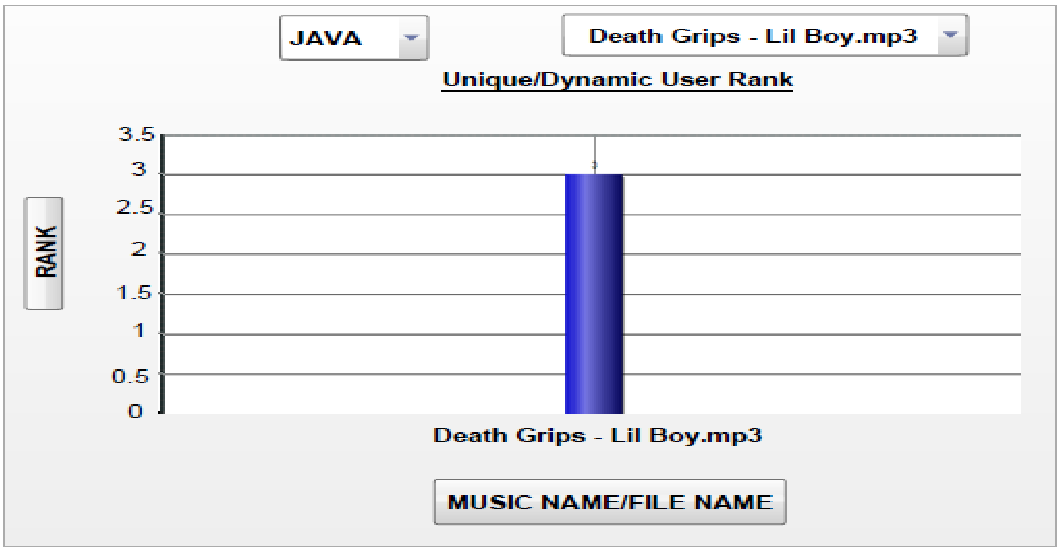
Security for Mobile Application and its D

Admin Log In

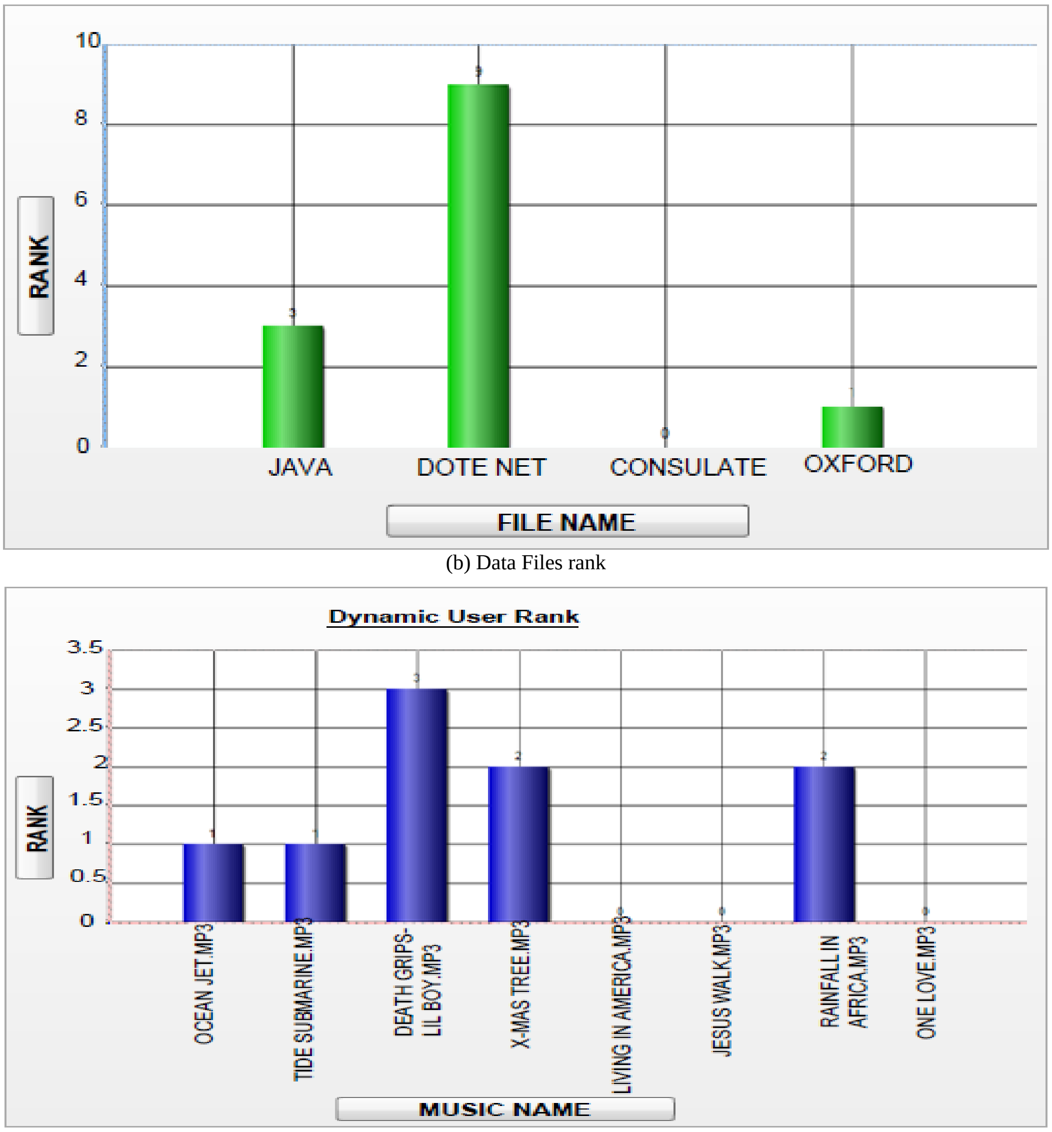
User Name : owner

Password : ••••

(b) End-user communication model within centralized mobile cloud security
Fig.6. Implementation of the system design



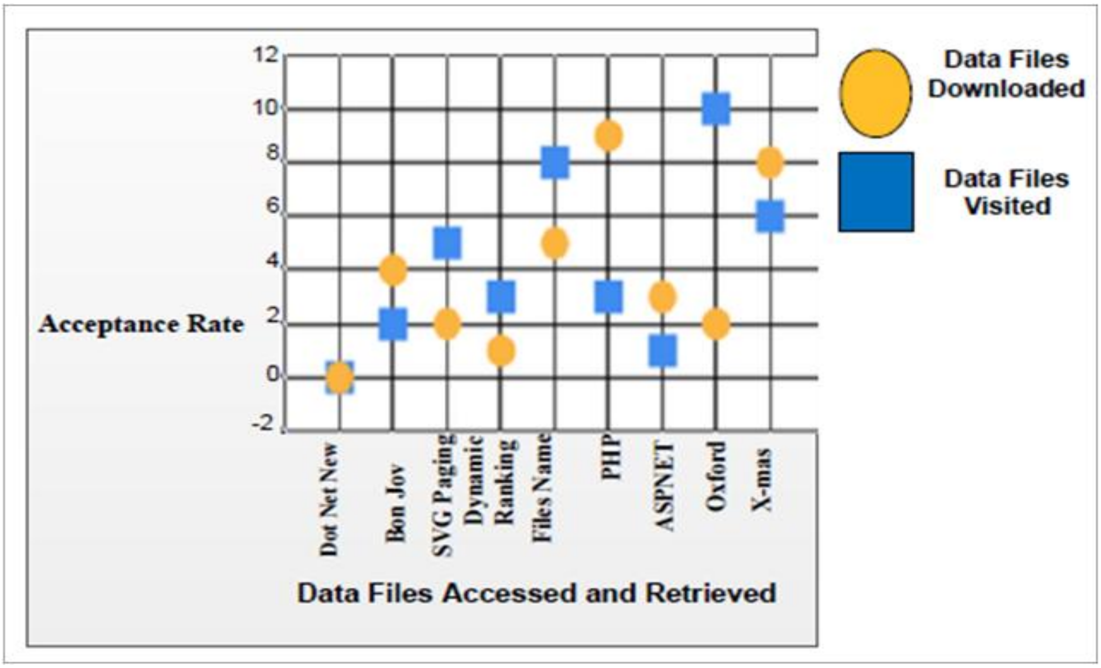
(a) Unique files rank and dynamic files rank



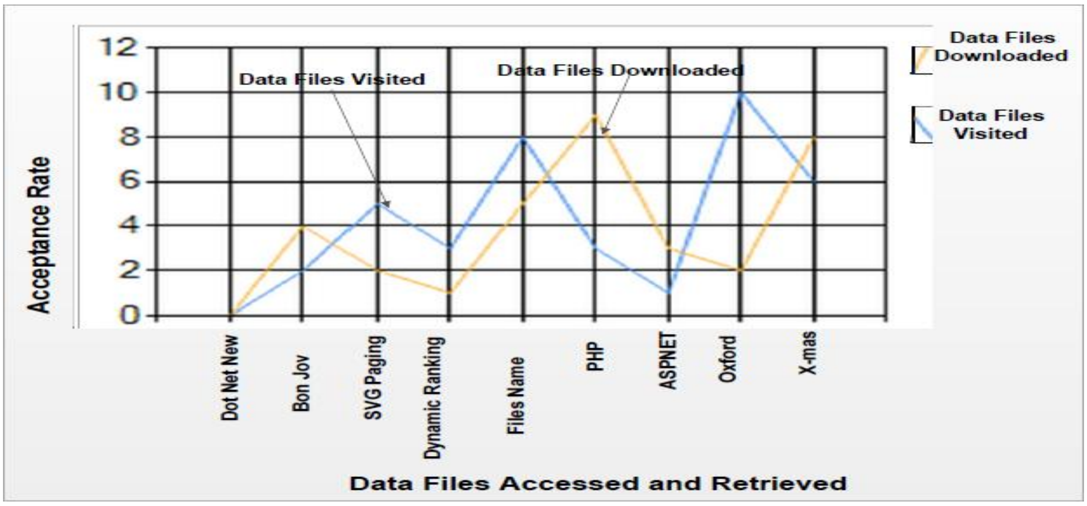
(b) Data Files rank

(c) Music files rank

Fig. 7. Data files access demand

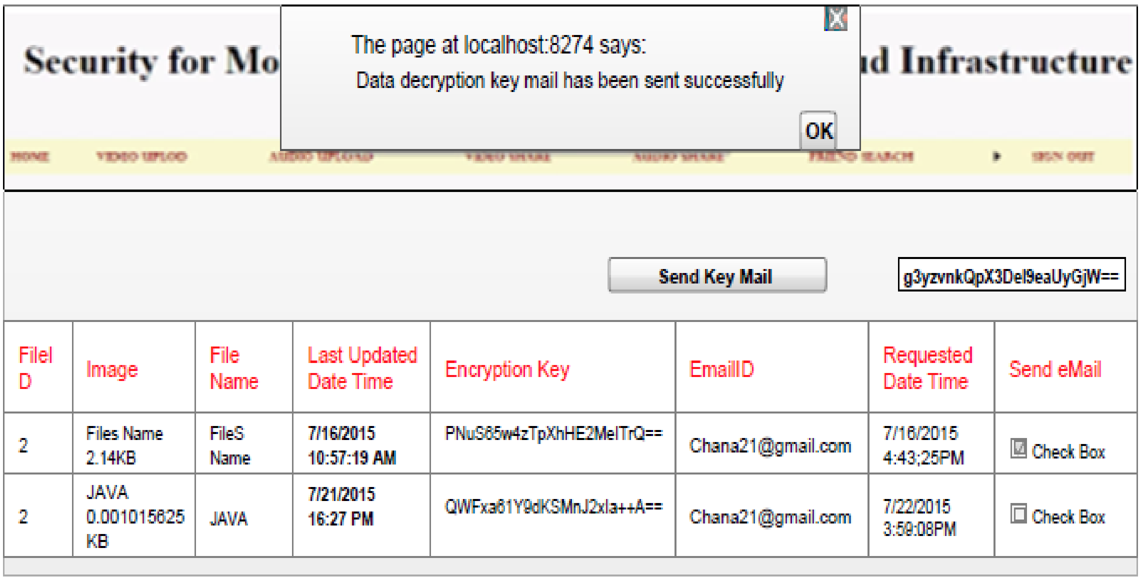


(a)Bubble



(b)Line

Fig. 8. Intents user search



The page at localhost:8274 says:
Data decryption key mail has been sent successfully

g3yzvnkQpX3Del9eaUyGjW==

FileI D	Image	File Name	Last Updated Date Time	Encryption Key	EmailID	Requested Date Time	Send eMail
2	Files Name 2.14KB	FileS Name	7/16/2015 10:57:19 AM	PNuS65w4zTpXhHE2MeITrQ==	Chana21@gmail.com	7/16/2015 4:43;25PM	☑ Check Box
2	JAVA 0.001015625 KB	JAVA	7/21/2015 16:27 PM	QWFxa61Y9dKSMnJ2xla++A==	Chana21@gmail.com	7/22/2015 3:59:08PM	☐ Check Box

Fig. 9. Data decryption key for data file recovery

Service Provider's Efficiency: service provider's efficiency influences how search request and retrieved data files are distributed and shared in the system over the internet. During the search process, the end-user (data user and data owner) can input multiple query keywords of interest. Typically, search requests usually consist of keywords such as "user name search", "school name search", "college name search", and "company-name search" from find user results list as shown in Figure 5 of part three. Data owner, who hosts data files after getting the search thread request and the requested demand of interest from data user, the hosts (data owner) has the rights for requested demand to accept or otherwise to distribute and share her/his data over the internet (in the system). Since cloud's admin manages screen capture, does key role/security assignment, auditing of the data files can done if unauthorized data users may search data files and try to distribute just before the data file has been accessed and retrieved. Figure 8 (Bubble and Stacked chart) shows data file retrieve and its acceptance rate for intent user search from data file results list that visited and downloaded by the end user.

Cloud's Admin Role on End-User Request Demand to Access Cloud Storage Services: since that, there is a system in place where the entities could communicate with each other in every data file access. Admin is trusted expert provide assistance on behalf of the end user upon request for any exposed risk of cloud storage services. In Figure 9 shows the end-user's lists and details of data files, encryption keys are stored in secure server. In the cloud's admin secure server, secure server managed by admin generates decryption key. The requested access to the data file's decryption operation requires cloud's admin to perform check-up in each end-user's data file requested demand to recover the data file. The decryption key is in the admin secure server auto-response in each data file session access request for recovery, and the decryption key can sent successfully to the corresponding end-user to recover the data file upon demand. But assign access role and authenticate end user is carried out by the cloud's admin. Significant importantly, shared data file and search-friend-request for data file sharing from the cloud server does not require involve admin in each friend request as well as data file sharing. cloud's admin clinking on send key mail button (admin secure server auto-response) as status display in Figure 9 was successful accomplished by selecting status list box (send mail) from end-user's data file add-list. In this paper, the purpose is to provide secure and safe infrastructure to the outsourced data files stored on the cloud serve. Importantly, ensuring and providing much stronger security guaranteed against adversary attack. Based on our proposed system we evaluate the following two different cases activities, i.e. data sharing from selected hosts, and search selected hosts (from friend request) for data sharing. We used this scenarios case to evaluate the reliable of our system design and the implementation if can influence security issue in positive or negative way. The end users access to the data files there is dynamic increment on the graph rank. There is access control for each end user and every data file the end-user access. This can attribute to variation in data files sharing and search a friend request to submit or receive new data file to share over the internet network. We observe this in Figure7 most of data files implemented has been shared that with the highest rank. The jump in the data file shared ranking varies with the number of end users increase and the positive impact of the shared data file. This means we expect that kind of data files can be vulnerable to the malicious attack or otherwise. In this concept, to ensure the confidentiality against any active adversary the communication secured using the IPSec authentication encryption class. To accomplish the security, IPSec introduced always correct when combined with any key to providing authentication encryption. Because once massage (data file) encrypted, the message is hiding inside the ciphtext during computation of tag of the ciphertext. We are locking the tag to lose the ciphertext. This process prevents anyone from producing the different ciphertext that will look valid and simply any modification be detected.

VI Conclusion

In this paper, we focus on outsourced data security problem in cloud infrastructure. The mobile cloud administrative management center includes key management, audit, assign access right, and access control rule. This user-centric management system allows data owner to have full control over their data files sharing by a end users authenticate by cloud's admin can upload, and delete data when required only for data owner. We proposed a system model and implemented the system existing works. Compared to the existing works for maintenance, we appropriate modified and improving to fit in current cloud storage security scheme for outsourced mobile application and its data. This proposed system can apply to access TCP/IP connection with different network access technologies. In this paper the end-user, access every data files at a fine-grained access control to protect data from unauthorized access. Data-files-at-rest and data-files-in-transit are maintained in a secure manner and providing sufficient security for the data files in the cloud-based server.

The proposed system and method provide both integrity and confidentiality (authentication encryption) to secure data file sharing in the existence of an active attack (adversary). Moreover, the proposed system solution provided access rights assigned to each data file deletion, also assigned to the role of the end-user and allow her/him to execute his access rights accordingly. The process prompts the end user to provide the user name and password accompanying with admin mail key (secure admin server auto-response send key) for assured deletion. In our future work, the system and proposed methods can extend by providing much stronger security than we have against an active adversary. Moreover, efficiency and performance run in polynomial time with the response of the methods with varying key and data file sizes can analyze. The results prove that existential propose system and methods can practically apply and solve an underline security problem in cloud infrastructure to secure data files in the cloud-based server. Based on the implementation of our system the limitation being some of the adversaries is more powerful. The system and the methods don't prevent replay attack and account for side channels (timing), which we consider in our future study.

Reference

[1] Bill Claybrook, "New River Marketing Research," Available online at:http://searchcloudapplications.techtarget.com.

[2] A. Pathak, Y.C. Hu, M. Zhang, Paramvi, Y.M. Wang, "ECE Technical Reports," Enables Automatic Offloading of Resource Intensive Smartphone Application. Purdue University (2009).

[3] "Apple iphone app store," http://www.apple.com/iphone/apps-for-iphone/.

[4] Apple-iCloud (2015) http://www.apple.com/icloud/.Accessed 13 August (2015).

[5] D. POPA, M. CREMEN, M. BORDA, K. BOUDAOUD," A security Framework for Mobile Cloud Applications,"*11th Roedunet International Conference (RoEduNet) Sinaia*, 2013, pp.1-4.

[6] S.Moran, "Security for Mobile ATE Applications," *IEEE AUTOTESTCON Proceeding USA*, 2012, pp.204-208

[7] The RSA Algorithm Engeny Milanov3 June 2009.

[8] X. Zhang, H.t.Du, J.q. Chen, Y. Lin, L.j. Zeng, "Ensure Data Security in Cloud Storage," *International Conference on Network Computing and Information Security*, 2011, pp. 284 - 287.

[9] Z.h. Xia, X.h. Wang, X.m. Sun, Q. Wang, "A secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud data," *IEEE Transactions on Parallel and Distributed Systems*, 2015, pp.1

[10] Zhenghua Lv, Huadog Meng, Tainyu Zhang, "A Cloud Platform for Distributed Spectrum Sensing," *Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, 2014,pp.1-4 .

[11] Dipayan Dev, Krishna Lal Baishnab, "A Review and Research towards Mobile Cloud Computing," *2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2014, pp.252 - 256.

[12] Dijiang Huang, Zhibin Zhou, Le Xu, Tianyi Xing, and Yunji Zhong, "Secure Data Processing Framework for Mobile Cloud Computing ",*IEEE INFOCOM Workshop on Cloud Computing*, 2011,pp. 614 - 618

[13] Q. Wang, C. Wang, K. Ren,W.j. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, 2011, V. 22(5), pp.847-859.

[14] P. Hazarika, V. Baliga, S. Tolety,"The Mobile-Cloud Computing (MCC) Roadbloacks," *Proceeding IEEE 4th International Conference on Wireless and Optical Communications Networks*, 2014, pp. 1-5.

[15] M. Klymash, M. Beshley, B. Strykhalyuk, T. Maksymyuk, " Research and Development the Methods of Quality of Service Provision in Mobile Cloud Systems," *IEEE International Black Sea Conference on Communication Network (BlackSeaCom)*, 2014,pp.160-164 .

[16] P. Urien, "Cloud of Secure Elements Perspectives for Mobile and Cloud Application Security," *IEEE Conference on Communication and Network Security*, 2013, pp.371-372.

[17] M. Al-Jarrah, A.K. R. Tamimi, "A Thin Security Layer Protocol over IP protocol on TCP/IP Suite for Security Enhancement," *IEEE Proceeding conference on Innovations in Information Technology*, 2006, pp.1-5.

[18] C.Gentry," A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.