International Journal of Research in Advent Technology, Vol.2, No.7, July 2014
E-ISSN: 2321-9637

Improve Data Security into Android Mobile with Cloud Computing Storage

Yogesh Peter Graham[1], Praveen Shende[2]
Computer Science & Engineering[1, 2],Chhatarpati Shivaji Institute of Technology Durg (C.G.), India[1, 2]
Email: yogesh.peter.graham@gmail.com[1], praveen shende@csitdurg.in[2]

Abstract-— Mobile cloud computing refers to the integration of the elements of mobile networks and cloud computing that offers best possible services for mobile users. It offers on request set of connections (network) way in to a shared pool of configurable computing resources (e.g., networks, servers, More Space about Data Storage, application, and services) that can be rapidly provisioned and released with least management effort or service provider interaction. The more and more information is located into the cloud by individuals and enterprise, protection issues begins to produce and rise. This paper discusses the different protection issues that occur about how protected the mobile cloud computing environment. The record of consideration for cloud computing security is recognized and discussed Encrypted mechanism to solve the Data Security issue

Index Terms: Mobile Data Security, Mobile Cloud Data Security, RSA Algorithms, Android Security, Encryption Decryption Data Security.

1. INTRODUCTION

This Potential benefits that includes cost savings and improved business outcomes can be offered by Cloud computing. It entails the accessibility of software, processing control and storage space on demand. It is before now a permanent match of consumer oriented services such as email, storage and social media [4]. The opportunities provided by cloud computing becomes available to enterprises of all sizes that enables them to deliver more scalable and durable services to employees, partners and clients at lower cost and with higher business agility [1]. Cellular cloud computing refers to the availability of cloud computing services in a Cellular surround. It incorporates the elements of Cellular networks and cloud computing, thereby providing best services for Cellular users. In Cellular cloud computing, Cellular devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the clouds [2, 5]. The more and more information that is placed in the cloud by individuals and enterprises, the more and more they become vulnerable to attacks and threats the Internet has to offer. The promise of cloud computing to gain fast access to business applications and boosting their infrastructure resources with reduced capital expenses put the business world into a more Challenges environment. A range of information security risks for cloud computing need to be cautiously considered. Risks vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud provider has implemented their specific cloud services. In this paper, we discuss the overview of cloud computing technology together with the Challenges and promises cloud computing and associated benefits. The different issues that arises with the emergence of Cellular cloud computing have been identified and discussed, thus drawing and realizing the security risks the cloud environment has to offer. This paper provides a list of considerations for cloud computing security that are needed to understand and assess the risks associated.

2. OVERVIEW OF CLOUD COMPUTING

Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as “a model for enabling suitable, on demand set of connections access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be apace provisioned and released with minimal management effort or service provider interaction”[11]. NIST give five exclusivity of cloud computing that describe and differentiate Cloud services from conventional computing approaches:

2.1 On-demand self-service involves customers using a web site or similar control panel interface to provision computing resources such as added computers, network bandwidth or client email accounts, without requiring human interface between consumers and the merchant.

2.2 Broad network access enables customers to access computing resources over networks such as the Internet from a wide collection of computing devices such as laptops and smartphones.

2.3 Resource pooling involves vendors using shared computing resources to provide cloud services to several clients. Virtualization and multi-tenancy mechanisms are typically used to both segregate and protect each customer and their data from other clients, and to build it appear to clients that they are the only user of a shared computer or software application.

2.4 Rapid elasticity enables the fast and automatic increase and decrease to the amount of available computer action, storage and network bandwidth as necessary by client demand.

2.5 Pay-per-use measured service involves customers only paying for the computing resources that they actually utilize, and being able to observe their usage. This is equivalent to household use of utilities such as electricity. Cloud services are often but not always utilized in concurrence with, and enabled by, virtualization technologies[6,7].

3. CLOUD SERVICE OFFERINGS

Cloud computing service offerings are broadly classified into three delivery models: the Infrastructure as a Service (IaaS); the Platform as a Service (PaaS); and the Software as a Service (SaaS) [1, 3, 4, 6].The Cloud computing services provisioning is shown in Fig-1. For SaaS, the service levels, protection, governance, compliance, and responsibility expectations of the service are contractually predetermined, managed and compulsory to the provider. For PaaS or IaaS, the end user system administrators has the responsibility to effectively control this issues, with some offset usual by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. It should be clear in also case that one can assign/transfer responsibility but not necessarily accountability for both consumers and providers.

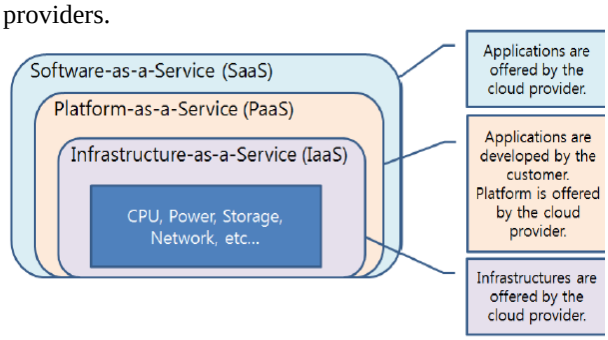

Fig. 1. Service Based Aarchitecture.

3.1 Software as a Service (SaaS) offers complete and finished software applications on require. A single request of the software runs on the cloud and services multiple end users or client organizations. It is a model of software use where an application is hosted as a service provided to customers across the Internet. By eliminating the require to mount and run the application on the customer's own computer, SaaS alleviates the client saddle of software maintenance, in progress process, and support. Example applications include email and an environment for users to collaboratively develop and share files such as documents and spreadsheets. These Client applications are in general accessed by users via web browser, eliminating the need for the user to install or maintain additional software. The provider controls and maintains the physical computer hardware, operating systems, software applications. The provider allows the client only to utilize its applications. mainly broadly used examples of SaaS consist of Gmail, Google Docs, and Salesforce.com.

3.2. Platform as a Service (PaaS) offers an operating system and can provide for every phase of software development and testing as well as suites of programming languages that users can use to develop their own applications. It provides a set of software and expansion tools hosted on the supplier's servers. PaaS enables clients to use the provider's cloud infrastructure to deploy web applications and other software developed by the customer using programming languages supported by the provider. Typically the vendor controls and maintains the physical computer hardware, operating systems, server applications. Typically the client just controls and maintains the software applications developed by the customer.

Commercial examples include Microsoft Windows Azure and Google App Engine, Force.com, and the Amazon Web Services Elastic Beanstalk.

3.3 Infrastructure as a Service (IaaS) offers end users direct access to physical computer hardware including CPU handing out, memory, storage, set of connections connectivity and other computing resources over the set of connections. It provides virtual servers with matchless IP addresses and blocks of storage on request. The provider may divide their hardware between multiple customers referred to as "multiple tenants" using virtualization software. IaaS enables customers to run operating systems and software applications of their selection. usually the vendor controls and maintains the physical computer hardware. Normally the client controls and maintains the operating systems and software applications. Examples of IaaS consist of Amazon Elastic Compute Cloud (EC2), Joyent, GoGrid, Rackspace Cloud, and IBM Computing on require.

3.4 Deployment Models for Cloud Applications

There are 4 basic cloud application deployment and consumption models that the Cloud computing architects must take into consideration: public, private, hybrid, or community clouds. Each offers

complementary benefits, and has its own trade-offs [1, 3, 4, 6, 11].

I) *Public Clouds:* Public clouds are owned and managed by Providers, and applications from altered clients are likely to be mixed together on the cloud's servers, storage systems, and set of connections. However, this model has a mixture of inherent security risks that need to be careful. A well architected private cloud correctly managed by a provider provides many of the benefits of a public cloud, but with improved control over security. Public clouds are most often hosted away from customer premises, and they give a way to decrease customer risk and cost by given that a stretchy, even temporary extension to enterprise infrastructure.

II) *Private Clouds:* Private clouds are client dedicated and are built for the exclusive use of one client, given that the extreme control more than data, security and valuable of service. The enterprise owns the infrastructure and has control over how applications are deployed on it. If the private cloud is properly implemented and operated, it has compact probable security concerns A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the provider, as an alternative of being required to accept the generic contracts designed for the consumer mass market that are offered by some public cloud providers. Private clouds may be deployed in an enterprise datacenter, and they as well might be deployed at a co-location service.

II) *Hybrid Clouds:* A Hybrid cloud involves a combination of both public and private cloud models. They can assist to supply on-demand, on the outside provisioned degree. The capability add to a personal cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. project Computing and private cloud expand external to consume public compute resource for peak need or deliver on manufacturing cloud. An example is using goods resources from a public cloud such as web servers to display non-sensitive information, which interacts with insightful facts stored or processed in a private cloud. Focus primarily on proprietary data centres, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

IV) *Community Clouds:* Community clouds are tailored to a specific perpendicular industry, such as government, healthcare or finance, present a variety of services, including infrastructure, saas or paas. It involves a private cloud that is shared by several organizations with similar security requirements and a need to store or process data of comparable sensitivity. This model attempts to acquire mainly of the security profit of a personal cloud, and most of the economic benefits of a public cloud. An example community cloud is the contribution of a private cloud by several agencies of the same government.

4. MOBILE CLOUD COMPUTING

The usage of cloud computing in combination with mobile devices is known as mobile cloud computing. It is a grouping between mobile networks with cloud computing, thereby given that most advantageous services for mobile users. Cloud computing exists when process and data are kept on the internet rather than on separate devices, given that on-demand access. Applications are run on a remote server and then sent to the user [2, 5]. Fig-2 shows an overview of the mobile cloud computing architecture.

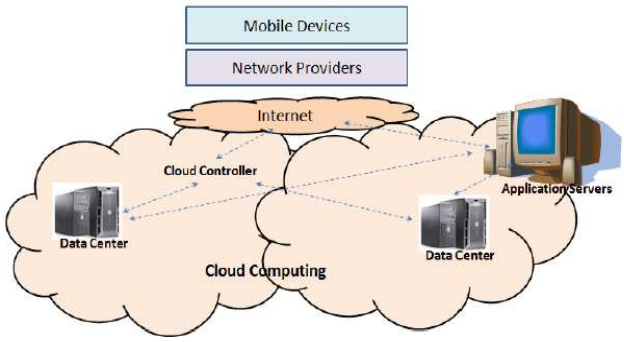

Fig-2 Mobile Cloud Computing Architecture

4.1 Mobile Cloud Computing Security

Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given concentration. Since mobile cloud computing is a grouping of mobile networks and cloud computing, the protection related issues are then separated into two categories: Mobile network user's security; and cloud security [8, 9, 10].

A) Mobile Network User's Security

Numerous security vulnerabilities and threats such as malicious codes are known to the different mobile devices such as Cellular, PDAs, cellular phones, laptops, and the like. a few applications to these devices can cause privacy issues for mobile users [10]. There are two main issues relating to the subscriber's security.

B) Security for mobile applications

The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. Other than mobile devices are controlled with processing and power boundaries, protecting them from these threats could be more difficult compared to normal computers. Numerous approaches have been developed transferring threat detection and security mechanisms to the cloud. Earlier than mobile users might use a certain application, it must go through some stage of threat appraisal. All file activities to be sent to mobile devices will be verified if it is malicious or not. as an alternative of running anti-virus software or threat detection programs nearby, mobile devices just

performs lightweight activities such as execution traces transmitted to cloud security servers.

1) Privacy: Providing private information such as indicating your current location and user's important information creates scenarios for privacy issues. The use of location based services (LBS) provided by global positioning system (GPS) devices. Threats for revealing confidential information could be minimized through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud. This leads to concerns that companies force use or sell this information as well as concerns that the information could be given to government agencies without the user's permission or knowledge.

2) Data Ownership: Another issue that arises from mobile cloud computing relates to the ownership of purchased digital media. with cloud computing it becomes achievable to store purchased media records, such as sound, video or e-books remotely rather than nearby. This can lead concerns concerning the true ownership of the data. If a consumer purchases media using a given service and the media itself is stored remotely there is a risk of losing access to the purchased media.

3) Data Access and Security: Related issues of access and security are significant to applications that rely on remote data storage and internet access in order to function. For example a user stores all of their calendar and contact information online, power outages can affect their ability to function from day to day. Mobile cloud computing is vulnerable due to multiple points at which access can be off and on (interrupted). Response and high speed availability can vary greatly for mobile devices utilized by the users.

C) Securing Information on the Cloud

Individuals and enterprises take advantage of the benefits for storing large amount of data or applications on a cloud. Though, issues in circumstances of their integrity, authentication, and digital privileges must be taken care of [10].

1) Integrity: Every mobile cloud user must ensure the integrity of their information stored on the cloud. each access they make must me authenticated and confirmed. Several approaches in preserving integrity for one's information that is stored on the cloud is being proposed. For example, each information stored by each individual or enterprise in the cloud is tagged or initialized to them wherein they are the only one to have access (move, update or delete) such information. Every access they create should be authenticated assuring that it is their own information and thus verifying its integrity.

2) Authentication: Different authentication mechanisms have been presented and proposed using cloud computing to secure the data access suitable for mobile environment. A few use the open principles and even supports the integration of various verification methods. For example, the use of way in or log-in IDs, passwords or PINS, validation needs, etc.

3) Digital rights management: Illegal distribution and piracy of digital contents such as video, image, audio, and e-book, programs becomes more and more popular. Some solutions to shield these stuffing from illegal access are implemented such as provision of encryption and decryption keys to access these stuffing. A coding or decoding platform should be prepared before any mobile user can have access to such digital contents.

5. MOBILE CLOUD COMPUTING WORKS

Typical services needed by mobile cloud client:

A) Sync

Sync service auto-synchronizes all state changes to App/Moblet Data back with Cloud Server.It supports several synchronicity modes such as both way sync, one way server sync, one approach device sync, time-consuming sync, and boot sync.

B) Push

Push service the service that manages state updates being sent as notifications from the Cloud Server. This improves the mobile user's knowledge as they do not have to pro-actively check for the new information.

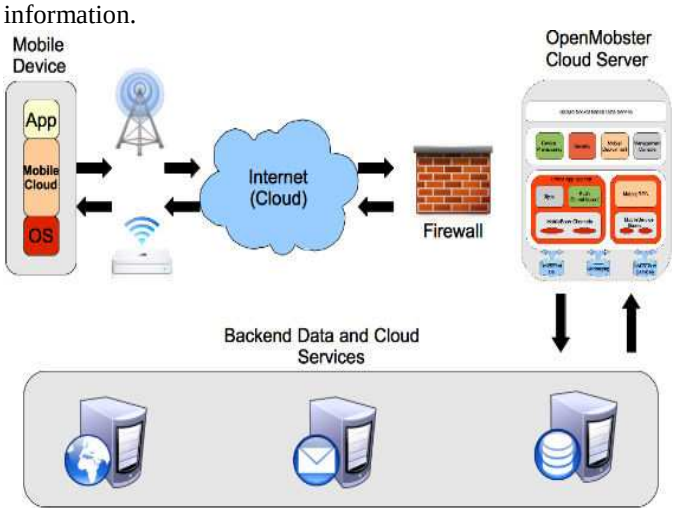

Fig-3 Architecture for Mobile Applications In Cloud Environment

C) OfflineApp

OfflineApp service provided is designed to be an App Developer's greatest friend. Its carries the organization capabilities to create smart coordination between the low-level services like Sync and Push. since of the OfflineApp service, the programmer never has to note down every code to actually to perform any synchronization. Synchronization is a little that is managed by the OfflineApp service and it decides which mode of synchronization is the best for the current runtime state of App. The App developer is never exposed to low level synchronization details

like both way sync, one way device sync, etc. It coordinates managing the Push service. It carries the stylishness to path the type of data being pushed along with which it is installed App on the device needs the notification. The App developers not write down any special code to receive the notifications. The instant the data way for the App is recognized, all synchronizations and move forwards Notifications are without human intervention handled by OfflineApp service.

D) Mobile RPC

Mobile RPC facilitates making synchronous RPC (Remote Procedure Call) invocations from the device to server side 'MobileServiceBean' components.

E) Network

Network service manages establishing a network connection with the Cloud Server. It manages the communication channel required to receive Push notifications from server. It carries smartness to track coverage and establishes proper connections without human intervention. This is a extremely low-level service and an App developer never has to deal with using directly. The App developer is shielded from any low level connection establishment, protection, procedure information, etc by using higher level Mobile Data Framework components.

F) Database

Database service manages local data storage details for the Apps. Depending on the platform in question it uses corresponding storage services. It is designed to synchronize storage between the suites of the Apps/Moblets installed on the device. It provides thread secure synchronized access to all Apps. Just like the Network service, its a low-level service used by Mobile Data Framework components.

G) Inter-App Bus

Inter-App Bus service provides low-level coordination/communication between the suite of Apps/Moblets installed on device.

6. MCC SECURITY CHALLENGES

A) Lack of control on resources and **multi-tenancy** of different users' applications on the same physical machine make cloud platforms vulnerable to attacks.
B) In addition to privacy issues, programs operation in the cloud are prone to:

1. **Tampering** with code/data/execution flow/Communication
2. **Masquerading**

C) Mobile code can navigate through multiple platforms before returning to the source, giving rise to the **end-to-end**

D) security problem, which involves decreasing control with every further hop in the chain of platforms.

E) Security mechanisms should satisfy the constraints of

1. **Real-time** response under intermittent network connection;
2. Keeping **communication costs** at minimum.
3. Incurring **limited computation overhead.**

7. RELATED WORK

Protected data processing mobile cloud infrastructure is highlighted in Fig-1. The mobile cloud is comprises three main domains: (i) the cloud mobile and sensing domain, (ii) the cloud trusted domain, and (iii) the cloud public service and storage domain. In this framework, each mobile device is virtualized as an ESSI in the cloud trusted domain and each ESSI can be represented as an SN in a particular application (a.k.a., a service domain). The Introduced ESSIs can be used to address communication and computation deficiencies of a mobile device, and offer improved security and privacy protections. A mobile device and its related ESSI can also act as a service provider or a service broker according to its potential, e.g., accessible computation and communication capabilities to support a particular communication or sensing service. This approach takes highest benefit of each mobile node in the system by utilizing cloud computing technologies. In this method, the cloud limit is unlimited to the customer device area. Note that an ESSI can be an accurate clone, a partial clone, or an image containing extended functions of the physical device. The set of connections between a user and its ESSI is through a secure connection, e.g., SSL, IPSec, etc. [12].

The scheme incorporates these two mechanism for providing confidentiality, access control as well as integrity to data. In this proposed scheme Trusted Authority (TA) who provides key to Data Owner (DO), generates an incremental message authentication code (MAC) of the file provided by DO. Now, when DO requests Storage Service Provider (SSP) for a file then after performing access policy, encrypted file is send to Decryption Service. Provider (DSP). DSP sends this file to DO as well as to trusted authority. Now TP again generates MAC of this received file and checks it for equality with previous MAC stored. If these two MACs are same then integrity of file is verified and the result is transferred to DO [13].

Liu et al. Projected to use hierarchical identity-based encryption algorithm to provide an resourceful sharing of the secure storage services in cloud computing. Here the encryption is used just the once and only one copy of the corresponding cipher text needs to be stored. It needs MD having higher computation ability. Wei et al. Proposed It is an auditing scheme used to secure cloud computing based on probabilistic sampling technique. Park et al. proposed a secure storage BLAST, which is improved

by a stream cipher rather than a block cipher with a novel block accessible encryption mechanism based on streaming ciphers [18].

8. PROPOSED WORK

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can reterive it. By securing the statistics, we are not allowing unauthorized access to it [19][20][21].

User data is encrypted first and then it is stored in the Cloud. When necessary, user spaces a appeal for the data for the Cloud provider; Cloud provider authenticates the user and delivers the information. RSA is a chunk cipher, in which each message is mapped to an numeral. RSA consists of Public-Key and Private-Key. In our Cloud surroundings, Pubic-Key is recognized to all, where as Private-Key is recognized only to the user who originally owns the data. Thus, encryption is completed by the Cloud service provider and decryption is done by the Cloud client or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the related Private-Key only. RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation must be done. This procedure is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: $d = e^{-1} (\text{mod } Ø(n))$ i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is $C = m^e \text{ (mod n)}$.
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the procedure of change the cipher text (data) to the original plain text (data).

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verity's the authenticity of the user and gives the encrypted data i.e., C.
3. The Cloud user then decrypts the data by computing, $m = C^d \text{ (mod n)}$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

9. EXPERIMENTAL RESULTS

In this section, we are taking some sample data end implementing RSA algorithm over it.

Key Generation:

1. We have chosen two distinct prime numbers a=61 and b=53.
2. Compute n=a*b, thus n=61*53 = 3233.
3. Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
4. Chose any integer e, such that 1 < e < 3120 that is coprime to 3120. Here, we chose e=17.
5. Compute d , d = e-1(mod Ø(n)), thus d=17-1(mod 3120) = 2753.
6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to the user.

***Encryption*:**

1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wishes to store the data.
2. Let us consider that the user mapped the data to an integer m=65.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user.C = 6517(mod 3233) = 2790.
4. This encrypted data i.e, cipher text is now stored by the Cloud service provider.

Decryption:

1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user then decrypts the data by computing, m = Cd(mod n) = 27902753(mod 3233) = 65.
3. Once the m value is obtained, user will get back the original data.

10. CONCLUSIONS

Cloud Computing is immobile a new and growing paradigm where computing is regarded as on-demand service. Once the organization takes the conclusion to move to the cloud, it loses control larger than the data. Thus, the quantity of shield needed to secure data is directly relative to the importance of the data. Security of the Cloud relies on reliable computing and cryptography.Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the information also, he can't decrypt it and obtain back the original data from it. Hence forth, data security is provided by implementing RSA algorithm.

REFERENCES

[1] Mahadev Satyanarayanan, "Mobile computing: The next decade," Proc. 11th Intl. Conf. on Mobile Data Management (MDM'10), Kansas, MO, 2010.

[2] "Amazon elastic compute cloud (EC2)." AWS. [Online]. Available: http://www.amazon.com/ec2/.

[3] Microsoft azure. [Online]. Available: http://www.microsoft.com/azure/.

[4] Google app engine. [Online]. Available: http://appengine.google.com/.

[5] D. Kovachev, D. Renzel, R. Klamma, and Y. Cao, "Mobile community cloud computing: emerges and evolves," Proc. 1st Intl. Workshop on Mobile Cloud Computing (in conjunction with) 11th Intl. Conf. on Mobile Data Management (MDM'10), Kansas, MO, 2010, pp. 393-395.

[6] A. Klein, C. Mannweiler, J. Schneider, and H. Schotten, "Access schemes for mobile cloud computing," Proc. 11th Intl. Conf. on Mobile Data Management (MDM'10), Kansas, MO, 2010, pp. 387-392.

[7] E. Marinelli, "Hyrax: cloud computing on mobile devices using MapReduce," Master thesis, Carnegie Mellon University, 2009.

[8] Cong wang ,Qian wang, and Kui ren ,Wenjing lou,"Ensuring data storage security in cloud computing" at IEEE(8-1-4244-3876-1/09).

[9] Dulaney E.,CompTIA Security+ Study Guide, Fourth Edition, Wiley Publishing Inc., Indiana,2009.

[10] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.

[11] Cloud computing methodology, systems and applications lizhe wang, rajiv.

[12] Booth.D,(2004).web service architecture.Retrived from http://www.w3.org

[13] Cong wang ,Qian wang, and Kui ren ,Wenjing lou,"Ensuring data storage security in cloud computing" at IEEE(8-1-4244-3876-1/09).

[14] F.A.Alvi, B.S.Choudary, N.Jaferry,"Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012).

[15] Security analysis of cloud computing: (http://cloudcomputing.syscon.com/node/1330353).

[16] Jagpal Singh,Krishnan lal and Dr.Anil kumar Shrotiya, Journal of Computer Science and Applications., ISSN 2231- 1270 Volume 4, Number 1 (2012), pp. 1-7

[17] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.

[18] Security analysis of cloud computing: (http://cloudcomputing.sys-con.com/node/1330353).

[19] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.

[20] G. Jai Arul Jose, C.Sanjeev, Dr. C.Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011.

[21] Jain Neha and Kaur Gurpreet "Implementing DES Algorithm in Cloud for Data Security" VSRD-IJCSIT, Vol. 2 (4), pp.316-321, 2012.

First Author

Mr. Yogesh Graham received the Msc (C.S) From Makhanlal Chaturvedi National University, Bhopal (M.P.) in 2009 And MCA from Punjab Technical University, Jalandhar in 2011 and pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India,. He is now attending the Mtech-CS course in CSIT and her research interest include Mobile Data Security with Cloud Computing and programming language (JAVA, ANDROID, PHP, ASP.NET), Cloud Computing and Web Development, OCJP certified.

Second Author

Mr. Praveen Shende, Asst. Prof.,CSE Dept. C.S.I.T. Durg, India, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, Presented 2 Natinnal conferences, 1 International conferences, 2 International journals. His interests are Programming Languages (Java, PHP, Joomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.