Cloud Security:Privacy and Data protection

Mihir Dhanani
Department of Computer Science and Software Engineering University of Canterbury
Christchurch, New Zealand
Email:msd54@uclive.ac.nz

I. INTRODUCTION

Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are cloud-based such as security as a service. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are a number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers of a public cloud service. This introduces an additional layer virtualization that itself must be properly configured, managed and secured. While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Cloud computing aims to provide convenient, on demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions (Mell and Grance, 2011). Cloud provides services in various forms: Software as a Service-SaaS (e.g. Google apps, 2011), Platform as a Service-PaaS (e.g. Google app engine (2011)), Microsoft's Azure (Azure services platform, 2011) and infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS); Eucalyptus, 2011; Open Nebula (Opennebula, 2011)).

II. RELATED WORK AND THREATS

Cloud services are provisioned through the Internet; security and privacy of Cloud services are key issues to be looked upon. International Data Corporation (IDC) survey (Gens, 2009) showed that security is the greatest challenge of Cloud computing. The recent Cloud computing security white paper by Lockheed Martin Cyber Security division (Martin, 2010) shows that the major security concern after data security is intrusion detection and prevention in Cloud infrastructures. Cloud infrastructure makes use of virtualization techniques, integrated technologies and runs through standard Internet protocols. These may attract intruders due to many vulnerabilities involved in it.

Cloud computing also suffers from various traditional attacks such as IP spoofing, Address Resolution Protocol spoofing, Routing Information Protocol attack, DNS poisoning, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS), etc. For e.g. DoS attack on the underlying Amazon Cloud infrastructure caused BitBucket.org, a site hosted on AWS to remain unavailable for few hours (Brooks, 2009). Computing-cost using current cryptographic techniques cannot be overlooked for Cloud (Chen and Sion, 2010). Firewall can be a good option to prevent outside attacks but does not work for insider attacks. Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in Cloud infrastructure to mitigate these attacks.

1. Intrusions to Cloud systems

There are several common intrusions affecting availability, confidentiality and integrity of Cloud resources and services.

1.1. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2) (Slaviero, 2009).

1.2. Flooding attack

In this attack, attacker tries to flood victim by sending huge number of packets from innocent host (zombie) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections.

In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via zombies. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability of the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of attack is called indirect DoS attack.

Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

1.3. User to root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him/her able to exploit vulnerabilities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target. There are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, keyloggers, etc.

In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.

1.4. Port scanning

Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules, etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning etc. In Cloud scenario, attacker can attack offered services through port scanning (by discovering open ports upon which these services are provided).

1.5. Attacks on virtual machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs. For e.g. BLUEPILL (Rutkowska, 2006), SubVir (King et al., 2006) and DKSM (Bahram et al., 2010) are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.

New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs) (NIST: National vulnerability database, 2011) that attract an attacker to gain access to hypervisor or other installed VMs. Zero-day exploits are used by attackers before the developer of the target software knows about the vulnerability. A zero-day vulnerability was exploited in the HyperVM virtualization application which resulted in destruction of many virtual server based websites (Goodin, 2009).

1.6. Backdoor channel attacks

It is a passive attack which allows hacker to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hacker can control victim's resources and can make it as zombie to attempt DDoS attack. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as Zombie to initiate DoS/DDoS attack.

Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above. To prevent attacks on VM/Hypervisor, anomaly based intrusion detection techniques can be used. For flooding attack and backdoor channel attack, either signature based intrusion detection or anomaly based intrusion detection techniques can be used.

III. IMPLEMENTATIONS

There are several objectives to be taken into consideration in order to host the cloud in a secure manner. One is authorization, i.e. only authorized users can login. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and,

conversely, many firewalls can perform basic routing functions. Three, The Apache HTTP Server Project is a collaborative software development effort aimed at creating a robust, commercial-grade, feature-rich and freely-available source code implementation of an HTTP (Web) server. Four, PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. PHP code is interpreted by a web server with a PHP processor module, which generates the resulting web page: PHP commands can be embedded directly into an HTML source document rather than calling an external file to process data. It has also evolved to include a command-line interface capability and can be used in standalone graphical applications. Five, Internet Information Services (IIS, formerly Internet Information Server) is an extensible web server created by Microsoft for use with Windows NT family. IIS supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP. Six, MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other 'AMP' stacks). LAMP is an acronym for "Linux, Apache, and MySQL. Seven, OpenSSL is an open-source implementation of the SSL and TLS protocols.

IV. EXPERIMENTS

The cloud used was Owncloud, hosted using IIS (Internet Information System) and Apache Server.
Tasks:

I. Apache, PHP, MySQL.
II. Server Side Encryption
III. OpenSSL
IV. Firewall

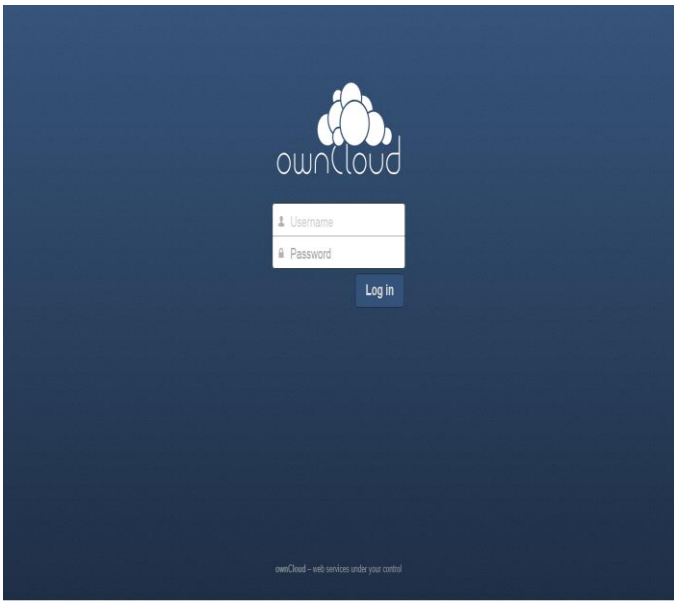
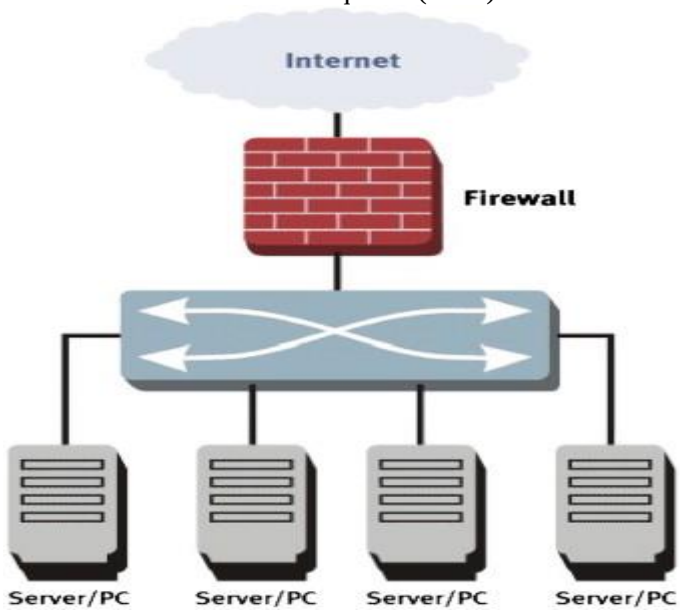


Figure 1 Owncloud Login

Firewalls: common solution to intrusions
Firewall protects the front access points of system and is treated as the first line of defense. Firewalls are used to deny or allow protocols, ports or IP addresses. It diverts incoming traffic according to predefined policy. Basic firewall installation is shown in Fig. 1 (2011, http://teleco-network.blogspot.com/), where it is installed at entry point of servers. Several types of firewalls are discussed in Sequeira (2002).



In Table 1, we summarize different firewalls used in network for security purpose. As firewalls sniff the network packets at the boundary of a network, insider attacks cannot be detected by traditional firewalls. Few DoS or DDoS attacks are also too complex to detect

using traditional firewalls. For instance, if there is an attack on port 80 (web service), firewalls cannot distinguish good traffic from DoS attack traffic.

Table 1.

Summary of Firewalls

Firewall Type	Summary
Static packet filtering firewalls	• Allow/deny packet by inspecting only header information such as source or destination address, port numbers etc. • Do not detect malicious code in packets and cannot prevent against spoofing and fragment attack
Stateful packet filtering firewalls	• Used in client server environment where client initiates request and server responses which are allowed in bypassing the firewall rules. • Requires additional resources like memory for state tables maintained in hardware or software
Stateful inspection firewalls	• Enhanced form of stateful packet filtering firewalls. • Used for applications like FTP where multiple ports are used and examine the payload and open or close the ports as per the protocol.
Proxy firewalls	• Can isolate internal network within Internet. Analyze the protocol syntax by breaking up client/server connection. • Require lots of network resources.

OpenSSL (https://localhost/owncloud)

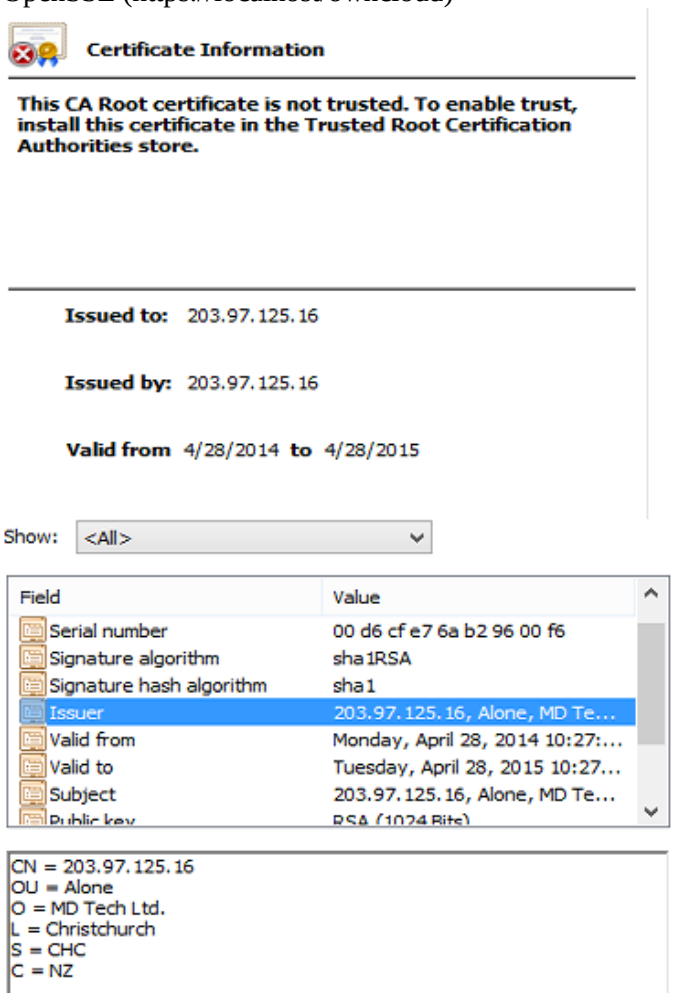


Figure 2 SSL Certificate

V. RESULTS

The results are divided into two parts.

1. When hosting using IIS alone

The result when hosting using the IIS is that the encryption when enabled doesn't crash the server unlike apache server. The encryption app is built on the more secure AES algorithm. The complete encryption is built on top of OpenSSL a well-known and tested encryption library. This means that the encrypt and decrypt happens transparently so that we can still use all the other features from like sharing, different viewer apps, WebDAV access etc, we use the users log-in password for encryption. This means that a user should choose a strong password in order to protect the data. It is important to know that by default a user will lose access to the data if he loses his log-in password. As an

additional feature the administrator can generate a recovery key which allows him to recover user data. Once this feature is activated in the administrator settings every user can enable the recovery key in his personal settings. By default the recovery key is disabled. Every user can decide for himself whether he wants this additional protection against password loss or not. Since we are using server-side encryption this feature does not reduce the security.

The encryption is based on three different keys: every user has a private/public key-pair, every file has a file-key and to give multiple users access to a file we have share-keys.

Every user has an asymmetric 4096-bit strong key-pair which consists of a private and a public key. The private key is encrypted with the user's log-in password, for the encryption AES-128 is used. Additionally there are up to two system-wide key-pairs: One for public link shares which allows ownCloud to decrypt files which are shared as public link and if enabled the recovery-key-pair.

In order to not always have to encrypt and decrypt large files we have introduced the file-keys which are 183 byte strong ASCII keys. The file-key is used to encrypt the users file symmetrically with AES-128. Than the file-key gets encrypted with the public keys from all users with access to the file. This means that if a user gets added or removed from a file we only have to re-encrypt the small file-key instead of the whole file.

Every time a file-key gets encrypted to multiple users OpenSSL generates for each user an additional share-key. Only the combination of the user's private key with the corresponding share-key enables the user to decrypt the given file again.

2. While hosting using apache server

The encryption app uses PHP's pear () which collides with the pear () of owncloud and makes the server crash, and is only resolved by disabling the encryption.
Except fot this all other features work similar to the hosting of IIS. Except for the synchronization among other devices. This works using apache server but access problems when using IIS.

VI. FIGURES

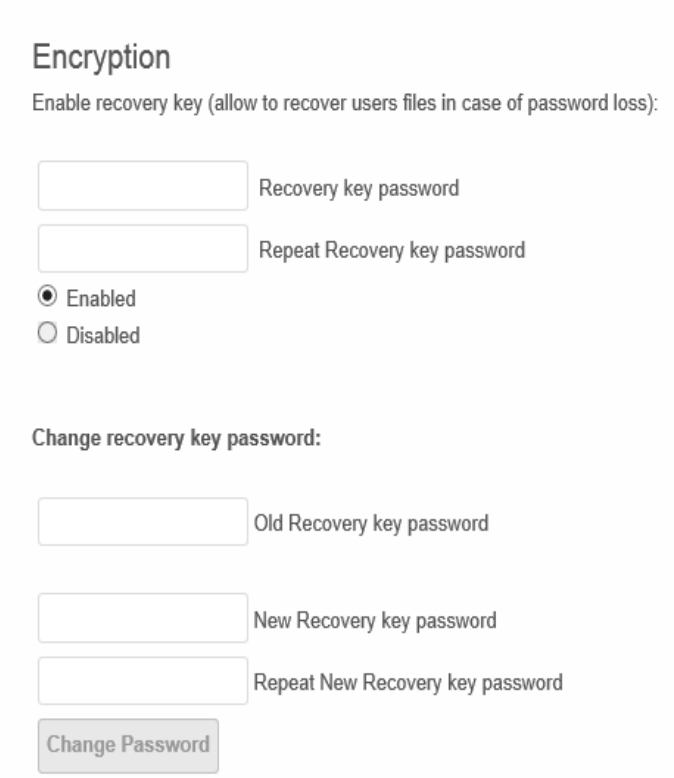


Figure 3 Encryption App

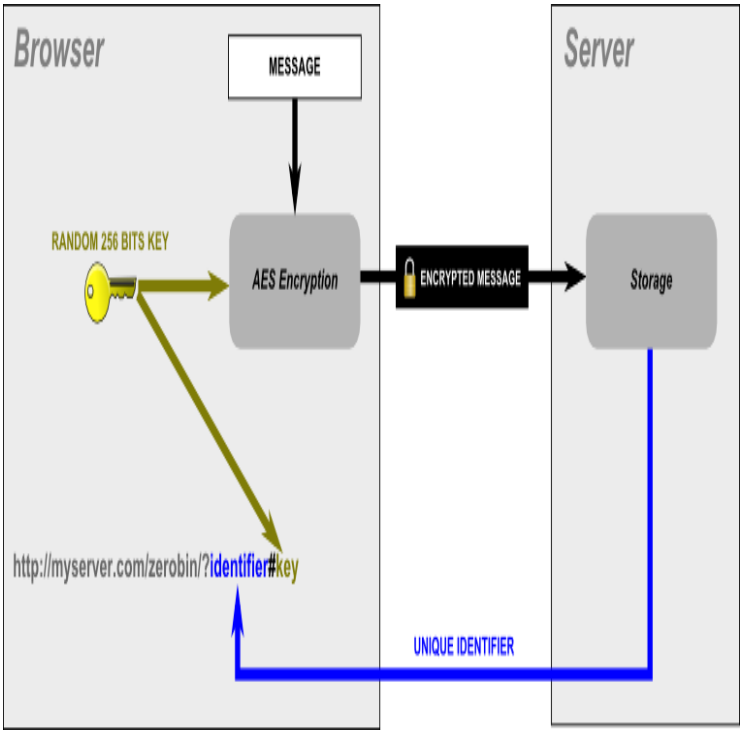
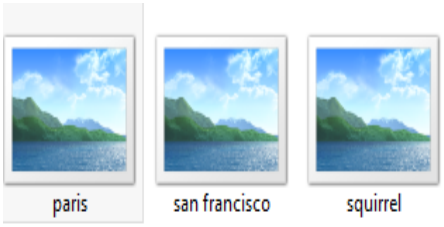


Figure 4 Encryption Structure

Figure 5 App for devices



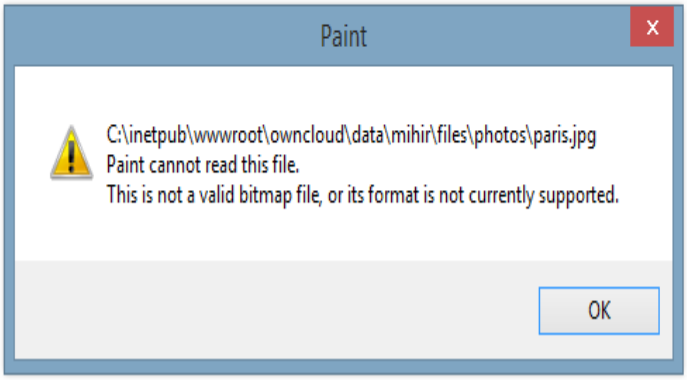


Figure 6 Access denied from server

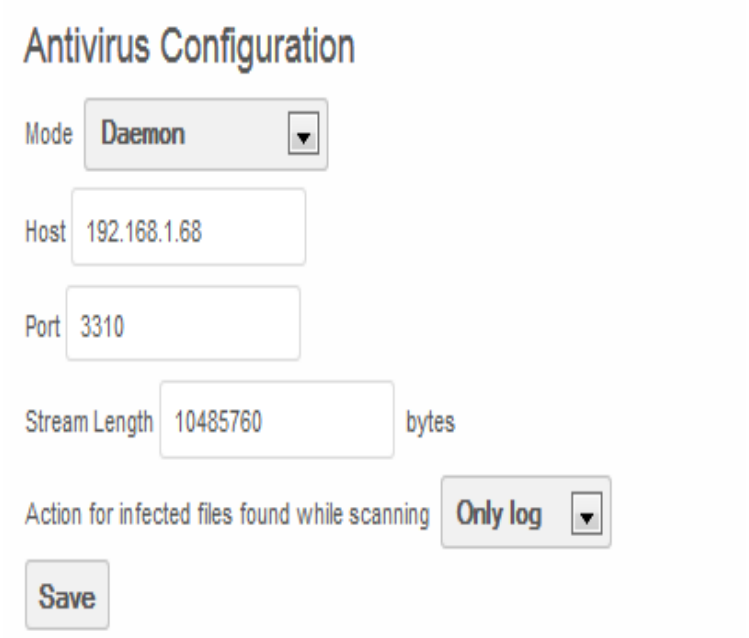


Figure 7 Antivirus app config

Figure 8 User management

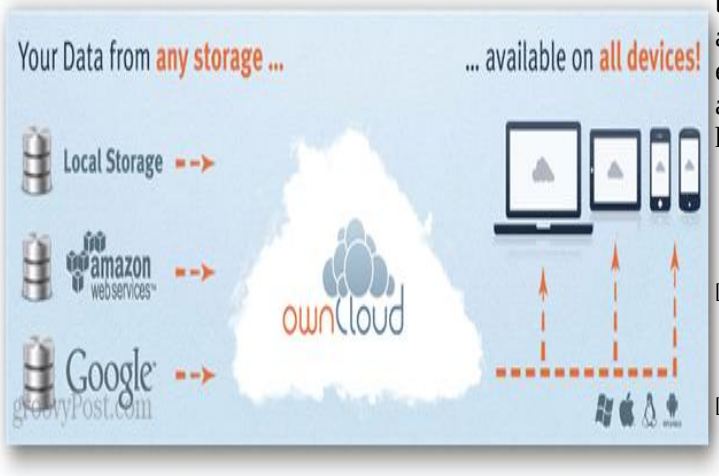
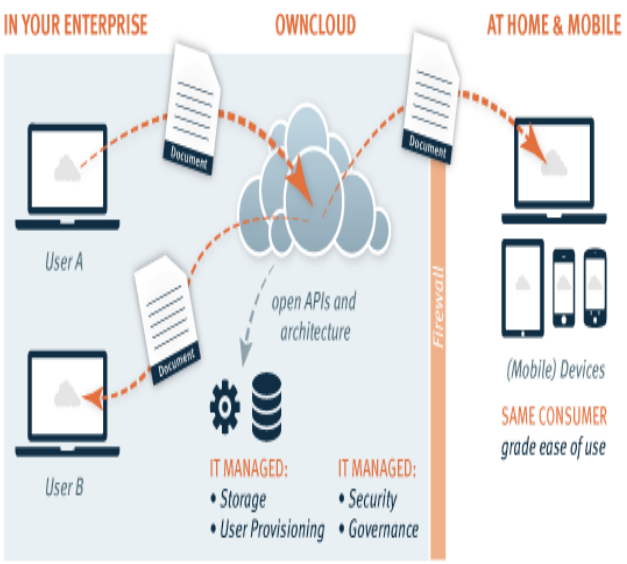


Figure 9 Overview



VII. CONCLUSION

In this paper, I used an open cloud source available as a host, in this case ownCloud and took measures in order to achieve the security requirement of the files being accessed from the server. My approach used server side encryption with a key management scheme, OpenSSL and firewall. This scheme is a good starting point and hopefully can be developed further in the future.

REFERENCES

[1] A survey of intrusion detection techniques in Cloud. Chirag Modi, Dhiren Patel, Bhavesh Borisanuya, Hiren Patel, Avi Patel, Muttukrishnan Rajarajan. Journal of Network and Computer Applications January 2013

[2] Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. Saman Zonouz,Amir Houmansadr,Robin Berthier,Nikita Borisov,William Sanders, Computers & Security, September 2013

[3] Shucheng Yu; Cong Wang; Kui Ren; Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," INFOCOM, 2010 Proceedings IEEE , vol., no., pp.1,9, 14-19 March 2010 doi: 10.1109/INFCOM.2010.5462174

[4] Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment Katarzyniak, Radosław E Chiu, Tzu-Fu E Hong, Chao-Fu E Nguyen, NgocThanh

[5] Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," INFOCOM, 2010 Proceedings IEEE , vol., no., pp.1,9, 14-19 March 2010

[6] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. 2009. Controlling data in the cloud: outsourcing

computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security

[7] Gartner: Seven cloud-computing security risks Jon Brodkin July 2008

[8] Cloud Computing Security International Journal of Engineering Science & Technology . 2011, Vol. 3 Issue 4 JAMIL, DANISH; ZAKI, HASSAN

[9] Cloud Computing Security Sean Carlin and Kevin Curran (University of Ulster, UK) Volume 3, Issue 1 2009

[10] Study on Cloud Computing Security FENG Deng-Guo,ZHANG Min+,ZHANG Yan,XU Zhen(State Key Laboratory of Information Security,Institute of Software,The Chinese Academy of Sciences,Beijing 100190,China)

[11] LIU Kai-hua,LI Xiong (Information Occupation Technique Institute of Hunan,Changsha 410001,China);Analyze the Security Model and Policy of Cloud Computing[J];Computer Knowledge and Technology;2011-08

[12] LI Song-tao,HU Heng-wu(Guangdong Medical College,Zhanjiang 524023,China);Application of Intrusion tolerance PKI in Cloud Database[J];Computer Knowledge and Technology;2011-17

[13] HUANG Hua(Qingyuan Polytechnic,Qingyuan 511500,China);Cloud Computing Security Key Technologies[J];Computer Knowledge and Technology;2011-23

[14] SHI Qiang,ZHAO Peng-yuan(College of Mathematics and Computer Science,Hebei University,Baoding Hebei 07 1002,China);Analysis of critical technologies on cloud storage security[J];Journal of the Hebei Academy of Sciences;2011-03

[15] CHEN Qin,MA Dan-dan,ZHANG Jin-man,DANG Zheng-qin(School of Computer Science and Technology,Hangzhou Dianzi University,Hangzhou Zhejiang 310018,China);Attribute-based encryption scheme with hidden access policy[J];Journal of Computer Applications;2011-11