Description of a Cloud Based Private Social Network Security Scheme

Yuncheng He

***Abstract*—As the internet of things permeates more aspects of life, the desire to access one's social network from whatever connected device available will become a requirement. Cloud-*based* personal data, remotely accessible from any connected device is evitable.**

This paper offers a solution to secure and assessable private social networks by creating a "Security Box" on which a private social *network* can provide safely distributed access. This access is managed, yet interactions are not burdened by onerous rules and membership overhead, that plague many private networks.

The Security Box is a cloud-based private social network security mechanism, implemented on a Amazon EC2/S3 cloud. The Security Box network provides multiple levels of security, enhanced *personal* and group encrypted files database, authorization control and 128-bit AES encrypted key management. Applying a Client/Server network model, the resulting private social network whose members enjoys a widely accessible shared database, suitable protected from unauthorized intrusion.

***Index Terms*—Cloud network, encryption, private social network, security.**

I. Introduction

Social networks are fundamentally public, cloud-based, internet-accessed, social interaction environments; potentially based on Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In the same manner in which cloud computing is transforming business economics and changing the way businesses gain access to sophisticated Internet services, social networks are changing the way businesses interact with their customers and the way people interact with each other.

Services such as Facebook®, Twitter®, and LinkedIn® are now migrating toward smart handsets, and in the future will further be compelled to migrate to every connected device where people desire to interact. As the "internet of things" becomes prevalent, social network integration and proliferation into every aspect of the connected world will follow. The benefit of having a Social Network migration occurring today to smart devices provides a microcosm for study to anticipate the hurdles faced for migration to all connected devices.

A. The Problems Facing the Proliferation of Social Networks

The biggest hurdle facing the proliferation of Social Networks is security. When a person or a business uses a public social network, a great deal of personal or proprietary information is being exposed to a public forum. Most social networks provide an implied contract that the information will be only used as the user sees fit. Unfortunately, this implication of security is often marketing misdirection rather than it is practical access control and security

It isn't news that social network user numbers around the world are growing at a fierce pace. From 2012 to 2013 social network use worldwide has increased by 18%, from 1.47 billion in 2012 to 1.73 billion in 2013. Almost one in four people the world uses a social network. At the current rate, by 2017, 2.55 billion will be using social networking [1]. Again it isn't surprising that by age group, social network use is skewed toward the young, but what is surprising is how popular social networks are with older people, indicating a proliferation beyond the tech savvy to general adoption. Percent of social network use by age group is as follows, 89% between the ages of 10-29, 78% between the ages of 30-49 and 60% between the ages of 50-64 and 43% between at 60+; where 40% of cell phone owners who use smart phone to visit social network site [2].

As use grows, as with all internet services, the concern for security is in lock-step with social network growth. Based on research of International Data Corporation in Fig. 1, security issues are the first priority concern of network users.

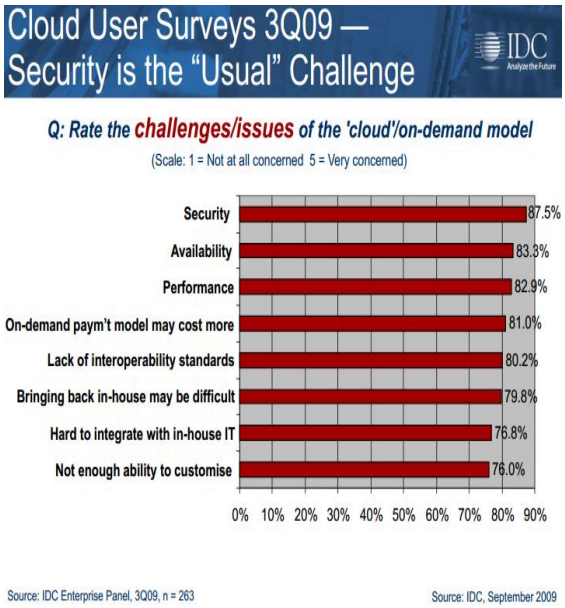

Fig. 1. IDC polling information [3].

The term "security" isn't a monolithic concept of concern; it encompasses various functions within the security eco-structure:

1) Confidentiality
2) Privacy

Manuscript received April 12, 2014; revised June 17, 2014.

Yuncheng He is with Northwestern Polytechnic University, USA (e-mail: chester@mail.npu.edu).

3) Filtered Notification
4) Information Integrity

1) Confidentiality

Confidentiality protects access to the user's data. In public social networks, one of the biggest problems users face is data being accessed or updated without a user's permission. The most common incidents of misuse of posted data is unauthorized access of social networking sites (43%), messages authored by someone other than the user sent to (25%) and change of personal data (24%).

Many social networking providers, such as Facebook®, give users the choice of who has access privileges, i.e. teens wishing to block prying parents, but these access protocols do nothing against the Social Media provider themselves from accessing client's data and using it as an equity asset or more directly selling the accumulation of data to marketing organizations as a revenue stream. User data protection is left to the integrity of the provider, which becomes a legal entanglement to enforce and generally impractical for most users to police or enforce.

2) Privacy

Privacy is a person's desire to control the access to the person (themselves) or others they associate with Privacy issues include identity theft, on-line predators, unintentional fame, stalking, unintended employment interaction and on-line victimization.

Unclear accessibility protocols can have unintended consequences for the unwary user. As an example, job recruiters reported negative reactions to finding profanity (61%), poor spelling or grammar (54%), illegal drugs (78%), sexual content (66%), pictures of or with alcohol (47%), and religious content (26%) on potential employees' social media pages [4]. The user posting this type of information would have most likely been more guarded had the intentions of the social network provider been clearer.

3) Filtered notifications

Social networking sites often send only good news. As an example, a site may only send out "positive" notifications to users. Facebook® will not send notifications to users when they are removed from a person's friends list. This is a form of censorship. The user is left largely uninformed about what the site is and isn't doing. Given social networking sites are a top news source for 27.8% of Americans, ranking below newspapers (28.8%) and above radio (18.8%) and print publications (6%) this practice of the public social network deciding for the user what should and shouldn't be seen could become a very large concern as social networks proliferates more devices [5].

4) Information integrity

The information on public social media may be false or unreliable. The information is only as good as the organization or people that provide it. There is no editor or watchdog of journalistic integrity, as with a newspaper. With public social media the ability to see false of misleading information is made greater given access is greater to wider variety of people and the ability for users to easily repost "news". As examples, On Sep. 5, 2012 false rumors of fires, shootouts, and caravans of gunmen in a Mexico City suburb spread via Twitter and Facebook caused panic, flooded the local police department with over 3,000 phone calls, and temporarily closed schools. Shashank Tripathi, tweeting as @ComfortablySmug, spread false information in the aftermath of Hurricane Sandy by tweeting that the New York Stock Exchange was flooding and that the power company would cut off electricity to all of Manhattan; the bogus information was picked up by national news outlets including CNN and the Weather Channel.

One doesn't have to look very hard for exhaustive discussions on the pros and cons of social media. These discussions are widely available on the Internet and proliferates the on-air news media. One example is the website, www.procon.org .

B. Private Social Networks: A Security Solution to Public Social Networks

Though a private social network restricts access to only like-minded individuals, there is still an overt need among users to control security directly. Below "Security Box" will be discussed as a method to control security within a private social network.

1) What is a private social network?

A private social network is an online community with some pre-defined affinity between the members that isn't necessary related to the network itself, though the network provides a forum of interaction for common purpose or interest. The business model is the most distinct difference between public social networks and private social networks. Generally, public social networks trade access to anyone in exchange to the provider to access the user's data; whereas private social networks charge fees to users and require some outside commonalty to be a member, but offer users the ability to more tightly control their data. In a large part, public social networks exist to mine revenue from the data their users provide while communicating with other users, whereas a private social network exists because users want a safe and secure forum of discussion and are willing to pay for this secure forum.

2) The benefits of private social networks

The level of security and trust are higher in a private social network because the reason the network exists is that there is an external relationship that motivated the creation of the network; trusted relationship between friends or colleagues. Further, since the members are paying to join and feel the connection is worth paying for, security policies, interaction policies and other network rules are defined and controlled by the users. The rules can't be effectively changed without user permission; trust and credibility through shared intention.

Further, given there is a preexisting relationship between users, this relationship is an authentication before joining the group and being privy to communications. Unlike a public social network, people you know may know others who you may not know, yet they have access to your information.

In a private social network, providing better security means users can define the levels and types of security they desire for their information and can discriminate who has access to the posted information. The rest of this paper will

discuss "Security Box" as a solution in providing private social networks with a method to control security within the network.

II. The Objectives of Security Box

The objective of this paper is to demonstrate "Security Box", a method to provide user-defined security on a cloud-based, private social network. This paper describes an efficient mechanism to 128-bit AES encrypt data, manage key distribution and storage, and authenticate users in order to protect personal data, or group member data, at a variety of user designated security levels in a private social network. A network employing Security Box will allow members to share their private information, comment on group activities, yet at the same time maintain control over the information they provide.

A. Design Architecture of the Cloud-Based Security Box

1) Research design

As a proto-type, this project sets up a cloud-based private social web server. Users can share their content on the server, assured that user's data is safely encrypted on the social server, though accessible to the authorized group. After finishing the proto-type testing stage, the application will employ a public cloud network(Amazon EC2/S3) for live testing. Each user will have their own unique account identity and common pass code to encrypt data on the server. Other subscribers will be granted access at various levels to view the data they are authorized to view.

2) Web server architecture

The web application employs a Presentation-Abstraction-Control (PAC) [6] architecture in Fig. 2 with a customized Model View Controller (MVC) architecture. The MVC is restricted to simple GUI's with one or more views on the same model. If the model consists of substructures, that all require their own special method of interaction, a more complex GUI architecture is required. The PAC architecture does not have the MVC model as its core component; rather it contains a hierarchical structure of PAC components. Each PAC component consists of the following items: Presentation, Abstraction, and Control.

Control is similar to the "Controller" described in the MVC architecture [7]. The Controller processes external events and updates the model. It also directly updates the Presentation part. It passes the changes being made to its parent PAC component. Abstraction contains the data, similar to that in MVC. However, the Abstraction element is a subset of the complete data structure of the application, and it does not play an active role in the notification of changes. The Presentation element displays information from the Abstraction element, as defined in MVC architecture.

3) Protocol used

HTTPS (Hypertext Transfer Protocol Secure) protocol is used create an encrypted secure link for transmitted data, between the user and the web server. HTTPS combines HTTP and SSL/TLS protocols together to create a secure communications tunnel between client and server. A server public key and authorization certificate method in Fig.3 is employed between client and server.

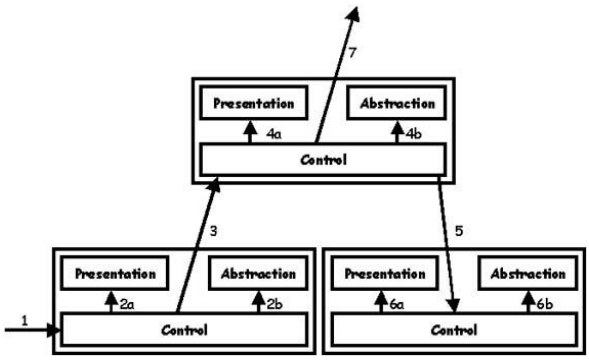

Fig. 2. PAC architecture model [7].

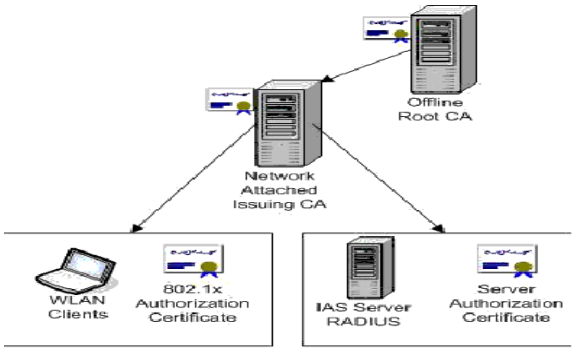

Fig. 3. Certification authority [8].

4) Encryption and decryption

A symmetric key [9] encryption and decryption process to encrypt file on web server is employed.

A symmetric key method is employed because it's easier for the user to control, than an asymmetric key method.

An Advanced Encryption Standard (AES) model in Fig.4 for encryption is employed, using a block size of 128 bits and three different key length: 128, 192 and 256 bits. AES is chosen because it's very secure and widely deployed.

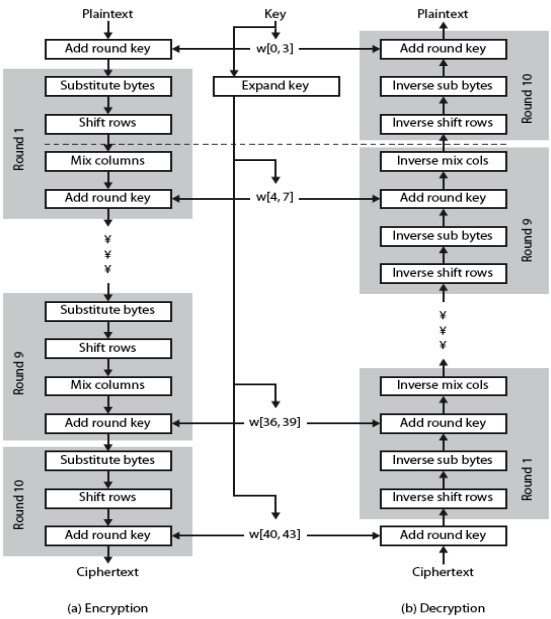

Fig. 4. AES encryption architecture [10].

5) File security levels

Because users post different types of information on a social network, some requiring very high security, where

other requiring less security, the user has the option to specify four security levels within the Security Box as follows:

a) Personal file security

This is the highest security level in which the encryption key will not be shared with others. The encrypted file cannot be decrypted by anyone except file owner. This is strictly secure data storage.

b) Group file security

This is a middle level security in which files will be encrypted / decrypted by a shared group key.

c) Group file sharing

This is a low security level in which only valid group users can read contents on web server.

d) Open file sharing

No security required. The content is open to all users.

6) Key management

a) Key management for personal file key

The key is generated based on user's personal information in Fig. 5, such as birthday or other unique information. This information is combined with a pass code from server to generate a unique encryption key.

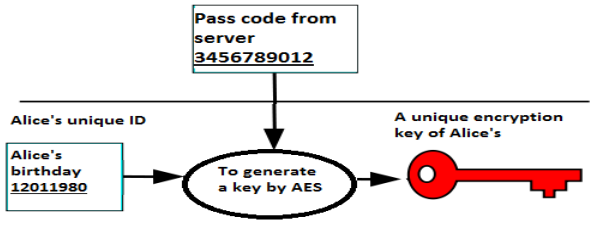

Fig. 5. Using personal identity and server generated passcode a unique key is created [11].

Encryption/Decryption: A unique aspect of the Personal File encryption is that the file can be encrypted/decrypted in Fig.6 by generating a unique key in real time. This added level of security reduces the risk of lost key, since keys are never saved.

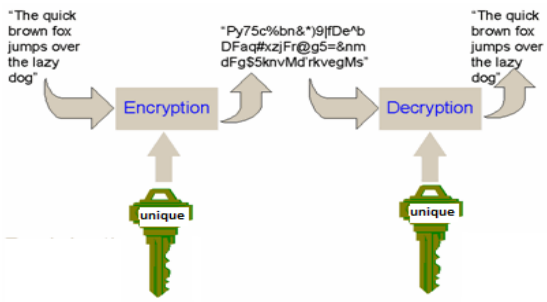

Fig. 6. Personal file encryption/decryption by unique key [12].

b) Group file security key management

Group File Security key management has three user selected modes:

- MODE 1

Key Generation: Using a group identity such as group name (CS670) or other unique ID in Fig. 7, combined with a pass code from the server, an AES encrypted group shared encryption key is generated.

Encryption/Decryption: Group File can be encrypted/decrypted by a generated group shared key in Fig. 8 without saving the key to reduce key lost risk.

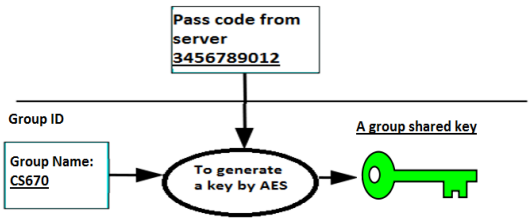

Fig. 7. Using group ID and a pass code to generate a group key [11].

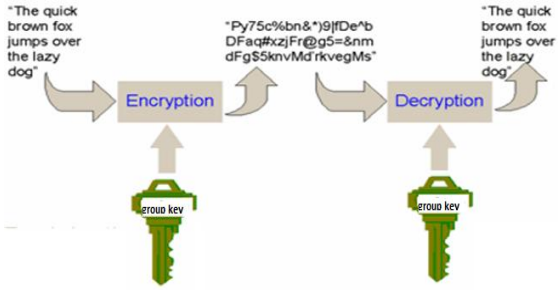

Fig. 8. Groupfile encryption/decryption without saving key [12].

- MODE 2

Key Generation: Using one group member's personal information and a passcode from the server to generate a AES encrypted key, which is distribute by email in Fig. 9 to the authorized group members.

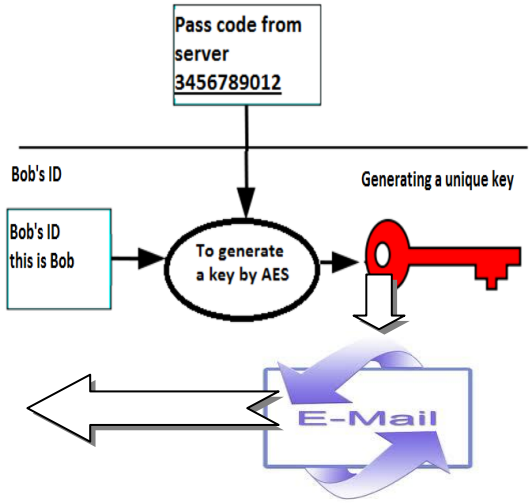

Fig. 9. Using one group member's personal ID and a pass code to generate a group key [13].

Encryption/Decryption: One group member becomes a master to generate and manage keys.

Group File can be encrypted/decrypted by receiving the key from the master's email in Fig. 10.

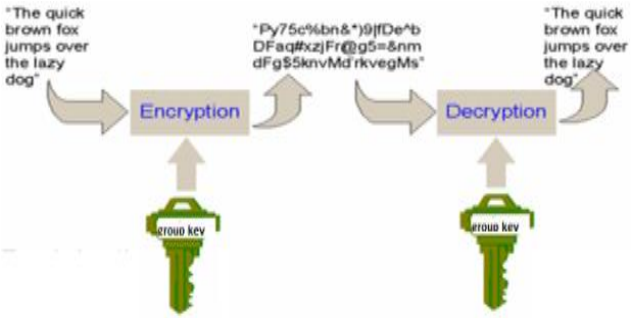

Fig. 10. Group file encryption/decryption by receiving a email from master's key [12].

- MODE 3

Key Generation: The passcode from server is used to generate the AES encrypted key directly in Fig.11. Additional security is provided because only valid users can read the passcode on server.

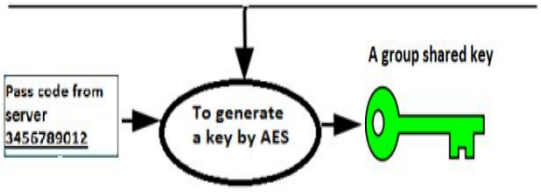

Fig. 11. Using a passcode from server only [11].

Encryption/Decryption: A group member can generate keys individually. Group File can be encrypted/decrypted by the generated key without saving the key to reduce key lost risk in Fig. 12.

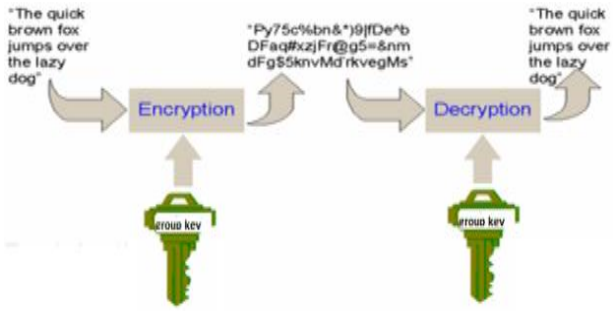

Fig. 12. Using a pass code from server only without saving key [12].

c) Group file sharing

Group members use their own username and password to log onto the server. Information at this general access level will be available to all group members. There is no file encryption at this level.

d) Open file sharing

At this level all files are openly shared and available for public viewing with no restrictions.

7) Authentication

Each user is registered in the server by either email invitation or self registration. A CAPTCHA in Fig. 13 is employed to protect against brute-force automated attack generating and inputting multiple combinations of passwords. CAPTCHA is implemented and employed together with username/password to authenticate a valid user.

Fig. 13. CAPTCHA Image [14].

8) Database Design

Each user has a unique identity within the Database in Fig.14. At the beginning, the user inputs personal information, such as first name, middle name, last name, gender, email address, photo (optional). Based on uid, a session is maintained open during the posting of comments, interests or encrypting files.

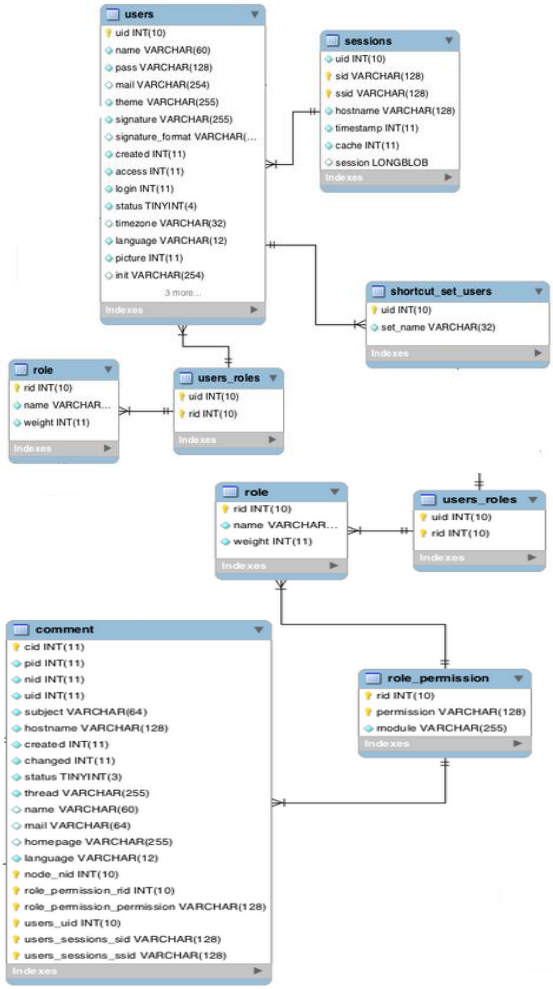

Fig. 14. Database [15].

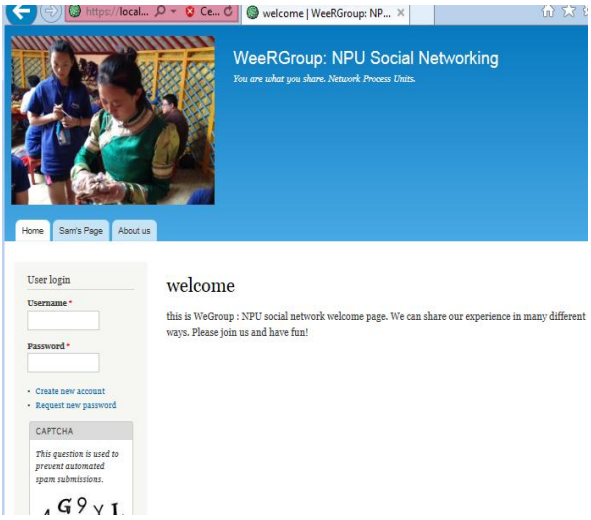

Fig. 15. Security box's login landing page [16].

9) Required resources

- Commercial cloud provider, such as Amazon EC2/S3, to provide access to scalable virtualized resources.
- Operation System: Linux (CentOS 6.0) or Microsoft Windows 2008
- PHP 5.4.22
- Notepad ++ v5.7
- MySQL sever 5.0.27
- Apache v2.2/Tomcat 7

III. Expected Result

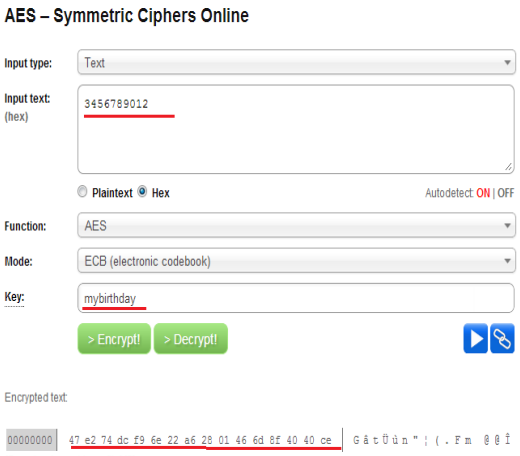

Fig. 16. Demonstration of how to generate an AES encrypted unit key [17].

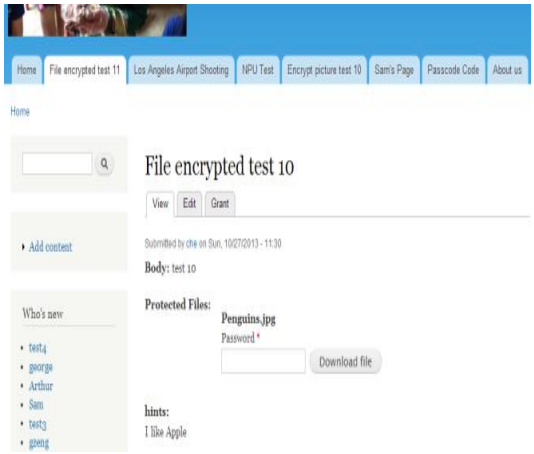

Fig. 17. Demonstration of key acquisition and decryption of encrypted server file [18].

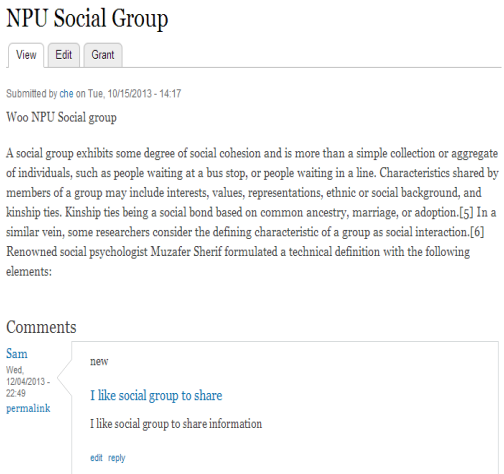

Fig. 18. Demonstration of group sharing comment in the clear [19].

When the project is completed, there are several expected results. First, the private social network can be deployed on public cloud network. Second, data transferring between client and server will be encrypted, resulting in a secure, encrypted database in Fig. 15. Third, the Security Box key management will be implemented with four security levels: 1). Personal File encryption with key management for individual files (Fig. 16 and Fig. 17 shows using personal id to generate a unique key, and using the unique key to encrypt/decrypt a file on server); 2). Group File encryption with key management for group offered secure content; 3). Group File sharing which is available to all authorized server users. 4). Open file sharing where files are in the clear and only require simple direct access to the web server which shows in Fig. 18. Lastly, the private social network will be protected against automated attack through a CAPTCHA.

References

[1] Social Networking Reaches Nearly One in Four Around the World. (June 18, 2013). eMarketer. [Online]. Available: http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976.

[2] Social Networking Fact Sheet Pew Research Centers Internet American Life Project RSS. [Online]. Available: http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/.

[3] E. Domage. (2010). Security: Trends IDC. [Online]. Available: http://uk.idc.com/downloads/security_briefing_pres.pdf.

[4] 2012 Social Job Seeker Survey. (January 1, 2012). Applicant Tracking System. [Online]. Available: http://recruiting.jobvite.com/

[5] K. Marino, "Social media: The new news source," *Infographic: Social Media: The New News Source*, April 16, 2012,

[6] P. Bergen. Presentation-Abstraction-Control. *Presentation-Abstraction-Control*. [Online]. Available: http://www.dossier-andreas.net/software_architecture/pac.html

[7] P. Bergen. Model-View-Controller. *Garfixia Software Architectures*. [Online]. Available: http://www.dossier-andreas.net/software_architecture/

[8] Microsoft. [Online]. Available: http://i.technet.microsoft.com/dynimg/IC226838.gif

[9] W. Stallings, "Symmetric encryption and message confidentiality," *Network Security Essentials: Applications and Standards*, 3rd ed., Upper Saddle River, NJ: Pearson Education, 2007.

[10] W. Stallings, "Advanced encryption standard," *Cryptography and Network Security: Principles and Practices*, 4th ed., Upper Saddle River, N.J.: Pearson/Prentice Hall, 2006.

[11] L18-encryption. [Online]. Available: http://cs.wellesly.edu/~cs110/OLD_WEBSITE/lecture/L18-encryption/public.jpg

[12] Buoni. [Online]. Available: http://www.cs.ucsb.edu/~buoni/cs8/labs/lab04/encryption4.gif

[13] Gstatic. [Online]. Available: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTGF3KAriurwU4JW5TLUL3qnz10HnFwkGPjQo3b8j9ItMYF9Hl20A

[14] Recaptcha-example. [Online]. Available: http://www.captcha.net/images/recaptcha-example.gif

[15] Drupal. [Online]. Available: https://drupal.org/files/er_db_schema_drupal_7.png

[16] Localhost. [Online]. Available: https://localhost/students/Created from owner's server

[17] AES-Symmetric Ciphers Online (AES Encryption - Easily encrypt or decrypt strings or files). [Online]. Available: http://aes.online-domain-tools.com

[18] File-encrypted-test-10. [Online]. Available: https://localhost/students/file-encrypted-test-10/created by author's server

[19] Localhost. [Online]. Available: https://localhost/students/created by author's server

Yuncheng Chester was born in China on June 21, 1964. He does live in San Jose, California, USA. He is a doctor computer engineering student in USA currently. He earned his master's degree in computer science in year 2001 in Northwestern Polytechnic University, Fremont, CA, USA and earned his bachelor's degree in electrical engineer in year 1986 in Northeast Dianli University, Jilin, China.

He has been working in Fortinet inc, located in 899 Kifer road, Sunnyvale, CA 94086 since January 1, 2002, a network security company from a startup to a worldwide public company as a Sr. manager of quality control currently. He has rich knowledge in computer networking and network security area. He has a plenty of working experiences from each individual function to system levels in hardware to software.