Social Media Security using Image Encryption

Prof.S.M.Rampur[1] Dhanshri D. Kadam[2] Akanksha B. Lull[3] Sandhya S.Mukare[4] Pooja R. Godse[5]
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]BMIT, Solapur, India

Abstract— Social Networks are becoming and integral part of people's lives. Students are spending much time on social media and are considered the largest category that uses application. social networking became a source of intelligence for advanced persistent threats and cyber criminals have shifted their focus toward targeting social networks for their attacks. This indicates that the nature of the use of social networks becomes a means for such threats to be able to move easily from one user to another. The proposed multimedia image sharing system includes Key Generation Center, Data Owner, Data User, Data Storing Center system entities that helps to share image securely using CP-ABE scheme. Here, specifically focus is on sharing image in '.jpg' format.

Key words: Social Media Security, Image Encryption

I. INTRODUCTION

Network and computing technology enables many people to easily share their data with others are using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified.

Attribute based encryption (ABE) comes in two flavors called key-policy ABE (KP-ABE) and cipher text-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners.

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time.

II. WORK CARRIED OUT FOR SOFTWARE PROJECT

Acquiring Domain Knowledge: A domain name is your website name. A domain name is the address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Computers use IP addresses, which are a series of number. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses.

A domain name can be any combination of letters and numbers, and it can be used in combination of the various domain name extensions, such as .com, .net and more.

The domain name must be registered before you can use it. Every domain name is unique. No two websites can have the same domain name. If someone type in it will go to your website and no one else's. www.yourdomain.com.

III. DECIDING THE ALGORITHM

Mancilla and Storer (2012) developed a stochastic scheduling problem considering waiting and idle time and overtime cost for operation room and surgery scheduling. A multi-stage stochastic integer program using sample average approximation was applied to solve this problem.

Erdogan, Denton and Gose (2011) also developed an algorithm to solve dynamic sequencing and scheduling of online appointments to a single stochastic server. The objective was to minimize patient waiting time (indirect and direct) and a clinic's overtime. In this study, it was assumed that service time and the number of customers to be served are uncertain. A special case of two customers was developed to provide some insights to show tradeoff between the cost of waiting time and likelihood of additional customers arriving. In this special case, the online system scheduled one 14 customer at a time until the capacity limit was exceeded for a particular day. A two sequencing decisions were assumed. One is first-come- first-served (FCFS). The other one is add-on-first-served (AOFS), in which the second (urgent add-on) customer arrives after the first customer but schedule before the first customer. Two-stage stochastic mixed integer program was proposed to solve the problem. After experimental analysis, they claimed that when all customers have the same cost and service time distribution, FSFC is better than AOFS. If indirect waiting costs are high for add-on customers, they should be scheduled first, otherwise they should be scheduled last.

IV. DECIDING DATA INPUT LOGIC AND PUT AT EACH STAGE

Input data in the simulation include the number of the two types of patients, who request an appointment each day and the patients' preference generation.

Patients' preferences are randomly generated as follows. For each patient, his /her preference is an array. The

numbers in this array represent the appointment days he/she prefers and the index of the array represents the order of preferred day. For example, [3, 4, 2] is one patient's preference list. It means that the first preferred day 28 for this patient is day 3 and second preferred day is day 4 and the third preferred day is day 2.

V. SELECTION OF LANGUAGE PROGRAMMING LANGUAGE: PHP

PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP reference implementation is now produced by The PHP Group. While PHP originally stood for Personal Home Page, it now stands for the recursive backronym PHP: Hypertext Preprocessor.

PHP code may be embedded into HTML code, or it can be used in combination with various Web template systems and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.

Standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

The PHP language evolved without a written formal specification or standard until 2014, leaving the canonical PHP interpreter as a de facto standard. Since 2014 work has been ongoing to create a formal PHP specification.

VI. SERVER: XAMPP

XAMP is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing purposes. Everything needed to set up a web server – server application (Apache), database (MariaDB), and scripting language (PHP) – is included in an extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server extremely easy as well.

VII. CODING

For our Project we are done the coding in PHP Language. PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. PHP code may be embedded into HTML code, or it can be used in combination with various Web template systems and web frameworks.

PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable.

And also we used the java scripting language for getting the online appointment scheduling. JavaScript is a "Client Side" programming language. This means JavaScript are read, interpreted and executed in the client which is our web browser.

VIII. IMPLEMENTATION DETAILS WITH PROCEDURES, CODING SAMPLE, OUTPUT:

A. Database: MYSQL

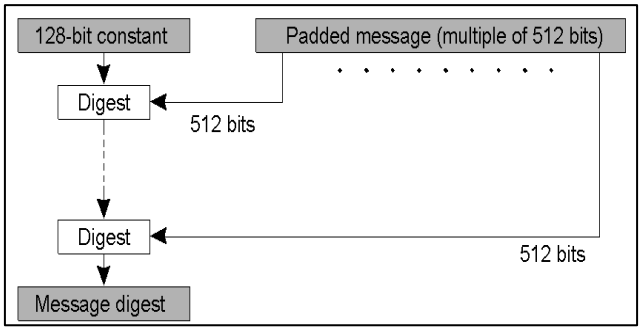
MySQL is an open-source relational database management system (RDBMS), in July 2013, it was the world's second most widely used RDBMS, and the most widely used open-source client–server model RDBMS. It is named after co-founder Michael Widenius's daughter, My. The SQL acronym stands for Structured Query Language. The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation. For proprietary use, several paid editions are available, and offer additional functionality.

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, MySQL, Perl/PHP/Python." Free-software-open source projects that require a full-featured database management system often use MySQL. Applications that use the MySQL database include: TYPO3, MODx, Joomla, WordPress, phpBB, MyBB, Drupal and other software. MySQL is also used in many high-profile, large-scale websites, including Google (though not for searches), Facebook, Twitter, Flickr, and YouTube.

IX. WEB BROWSER: GOOGLE CHROME

Google Chrome is a freeware web browser developed by Google. It used the WebKit layout engine until version 27 and with the exception of its iOS releases, from version 28 and beyond uses the WebKit fork Blink. It was first released as a beta version for Microsoft Windows on September 2, 2008, and as a stable public release on December 11, 2008. As of December 2015, Stat Counter estimates that Google Chrome has a 58% worldwide usage share of web browsers as a desktop browser. It is also the most popular browser for smartphones, and combined across all platforms at about 45%. Its success has led to Google expanding the 'Chrome' brand name on various other products such as the Chromecast. Google releases the majority of Chrome's source code as an open-source project Chromium.

X. ALGORITHMS



XI. ALGORITHM STEPS

A. STEP1: Append Padding Bits

The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512.

Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. At least one bit and at most 512 bits are appended.

B. STEP2: Append Length

A 64-bit representation of the length of the message is appended to the result of step1. If the length of the message is greater than 2^64, only the low-order 64 bits will be used.

The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words.

C. STEP 3: Initialize MD Buffer

A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98

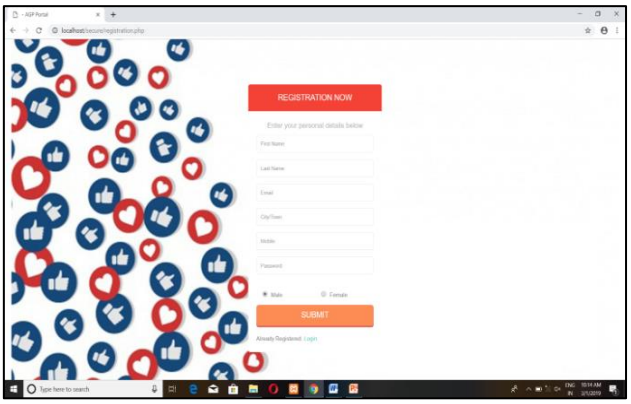
D. Step4. Process Message in 16-Word Blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

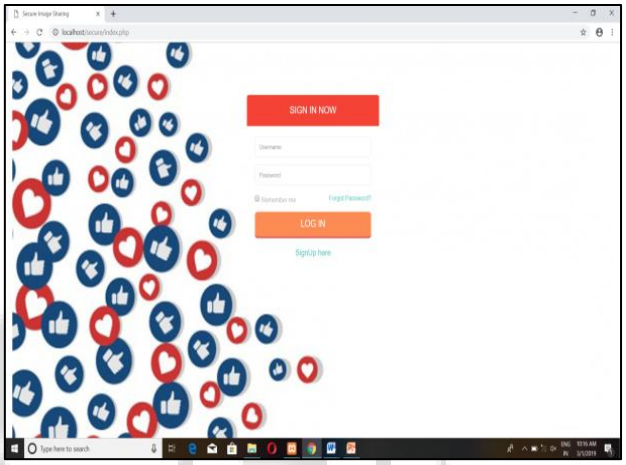
F (X, Y, Z) = XY or not (X) Z
G (X, Y, Z) = XZ or Y not (Z)
H (X, Y, Z) = X xor Y xor Z
I (X, Y, Z) = Y xor (X or not (Z))

XII. SNAPSHOT

A. Registration



B. Login



XIII. CONCLUSION

Social media is used by millions of individuals who collectively generate an array of social forms from their interactions. Social media network maps can be useful in understanding the variety of social structures that emerge. Network maps can reveal the structures of the crowd and highlight strategic locations or roles in these webs of connection. By mapping social media network spaces, researchers and practitioners can learn about the most common and best uses for these communication services.

REFERENCES

[1] J.-M. Zhu and J.-F. Ma, "Improving Security and Efficiency in Attribute Based Data Sharing," IEEE Transactions on knowledge and data engineering.
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10s 2010.

