Hybrid Algorithm for Web Based Social Network

S.Thiraviya Regina Rajam
Research Scholar,
St.Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, India.
Srajicic10@gmail.com

Dr.S.Britto Ramesh Kumar,
Asst.Professor, Dept. of Com.Science,
St.Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, India.
brittork@gmail.com

Abstract **- Security is the one of the biggest concern in different type of networks. Due to diversify nature of network, security breaching became a common issue in different form of networks. Solutions for network security comes with concepts like cryptography in which distribution of keys have been done. As Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we are focusing on security enhancing by enhancing the level of encryption in network. This study's main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques. In our research we have proposed a combination of RSA and MD5as a hybrid link for Web Based Social Network..**

Keywords: RSA, Message Digest, Encryption.

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great

non repudiation deals with signature. Security in networking is based on cryptography Encryption is the vital part of information sharing so we have put our efforts into encryption area for RSA algorithm with authentication

powered by MD5 security so that we can make security harder by giving a hybrid algorithm.

II. EXISTING SOCIAL NETWORK MECHANISM / APPROACHES

In this section, different approaches will be presented in details.

Tsai et al(2010) proposed the proxy–based real time website security protection mechanism uses the concept of Cloud Computing and its main function is detecting the websites security threats[1]. The concept is to combine several online security scanning services and protection

importance because of intellectual property that can be easily acquired through the internet.

The privacy requirements normally encountered in the traditional paper document world are increasingly expected in Internet transactions today. So with the rapid spread of digital communication networks, there is great need for security and privacy of transmitted data. Therefore, the methods of securing information are becoming a major issue, for which the encryption and decryption systems have been created. Secure digital communications are necessary for web-based e-commerce, mandated privacy for medical information, etc. Many hardware and software protocols have been implemented to improve the security of information, but the only true method of securing data is to encrypt it. The national and societal view of the role of encryption will be one of the defining issues for our culture in the twenty-first century. Network security problems can be divided roughly into four intertwined areas: Secrecy, Authentication, Non repudiation and Integrity control. Secrecy has to do with keeping information out of hands of unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information

software to scan a webpage's security.. This approach improves and develops the scanning correction rate, and it prevents users from accessing security compromising websites.

Graffi et al(2009) introduced Social Networking Sites that are web-based platforms consisting of millions of users and participants in social networks sites[2]. Security framework for P2P-based platforms for SN supports the users' registration and login process, where a new user chooses a unique username and password to generate an asymmetric key pair Private key, Public key. In addition, it supports access control as different users have different access rights such as reading shared items, creating new shared items, and altering existing files.

Durr et al (2010) proposed Re Socializing Online Social Networks[3]. There are several requirements for SN users that needs to be carefully analyzed. These include information, self determination which requires that users'

profiles and personal content may not be disclosed to any other users than the trusted contacts. As a result, all communication must ensure security against man in the middle attacks. A manageable secure mechanism is also required to publish a selected profile attributes depending on the trusted contacts, control profile personal data, and the ability to terminate the user's own online SN account. A novel decentralized multi-domain SN was designed. Multi domain SN is based on categorizing the SN into the following three domains: social Webspace, SocialMobilespace, and Social Homespace. To connect with other users there are two proposed basic schemas which are out-of-band invitation (OOB) and coupling.

Hogg et al (2009) introduced Security challenges for Reputation Mechanism using SN Sites[4]. The Reputation Mechanism is a part of a recommendation system used as both a main component in peer-to-peer transactions and in online SN by allowing users to personalize recommendations via users they trust.

Shin et al (2009) introduced a framework for enhanced User –Control persona in OSNs [5]. The U-Control framework enables the main services such as **(1)**Identifying Attribute Management by giving a privacy numerical rating from 1 (least sensitive) to 5 (most sensitive) for each user attribute. **(2)** Selective Attribute Disclosure and Sharing using an ordered skip list to search and update an element (x) using three operations *find(x)*, *insert(x)*, and *delete(x)*.

Ho et al(2009) proposed security protection issues in SN Sites[6]. The main purpose of SN sites is sharing information and keeping in contact with users of different relationship levels such as Best Friends, Normal Friends, Casual Friends, and visitors. This approach helps users to determine their required privacy levels, and have a good amount of information about the future potential risks in different activities.

Diaz et al(2009) proposed Social Application in the Home-Network[7]. The SE is an intermediary between the SN site and the user to ensure the correct representation of the across the different devices. The SW is responsible for the security and privacy issues in the request communication. It provides credentials for the devices as well as parental controls.

Anderson et al (2011) introduced Privacy-Enabling Social Network[8]. This model protects users' information not only from unauthorized users, but also from the network operator. To adapt the simplicity of the centralized server, it makes it impossible to prevent that server from analyzing the traffic in the controlled network.

Batch et al (2009) proposed Identity Server and Anonymous Identifier in Mobile Social Networks[9]. This approach provides certain functions that link a user anonymously to use in third-party applications. By that, the user's identity will be hidden while requesting information and applications from SN sites. This privacy protection can take place when adapting while using a third-party application.

Mathewet al (2010) proposed a framework Reputation for Directory Services (ReDS)[10]. To secure directory services in open P2P systems a Reputation for Directory Services (ReDS) framework for using reputation management to improve and enhance the security of locating information in distributed systems, has been proposed. Reputation for Directory Services has been applied to Salsa to be Salsa-ReDS which takes advantage of the redundant lookups and the ability of the requesting node to identify the correct result. The local contacts which provide correct results gain positive reputation, and those nodes which provide incorrect results gain negative reputation, so it will be easy to identify the reliable local contacts and the malicious nodes.

Carminati et al (2009) proposed Semantic Web Based Framework Online Social Networks.[11]. It includes lot of personal information which leads to opportunities and challenges. The Resource Description Framework (RDF) and the Web ontology language (OWL) have been used for Modeling SN data. It models the following five important aspects of SN sites: Modeling Personal Information, Modeling Personal Relationships, Modeling resources, Modeling User/Resource.

III. PROBLEM FORMULATION

An Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we have focused on security enhancement by enhancing the level of encryption in network. For required research we have worked on well-known encryption algorithms RSA with MD5. We have proposed the hybrid algorithm for RSA Algorithm with digital signatures powered by MD5 security with a small case study of applications for this hybrid algorithm.

IV. OBJECTIVES OF THE STUDY

- To study the issues of Security for Different networks. To Harden up the Encryption Process for Network Security
- To study the already implemented algorithms for public key exchange in communication of data

□□□□□□□To provide a stable encryption, this can make good communication without carrying about data integrity threat.

- To test the performance of web Based Social Networks for proposed experiment.

V. RESEARCH METHODOLOGY

To achieve the set objectives, our research focused on the performance measurement of network structure with implementation of Different security algorithm. We have considered RSA and MD5 algorithm for checking response time, load, throughput and reliability of Social Networks with implementation of these algorithms. Our research focused on these algorithms implementation in four Phases.

1st Phase: This phase contains the layout of framework .

2nd Phase: This phase contains the basic functionality of framework .

3rd Phase: In this phase, we have implemented the different scenarios and different scenarios including a scenario without any security algorithm, a scenario with RSA algorithm (RSA, MD5).

4th Phase: Results from all Scenarios have compared with proposed algorithm) to fetch parameters like Overall Throughput, Response time and load.

VI. PROPOSED FRAMEWORK

6.1 proposed framework

To solve the problems with traditional username password authentication, alternative authentication methods, such as Graphical Password have been used which allowing user to choice stronger password by click on images rather than type alphanumeric characters. It's easy for user to remember his password and too difficult for attackers to guess the password. The proposed framework is a new design and more secure graphical password system, called two factor framework for user authentication.

The proposed framework proposes the concept of creating graphical password to provide secured authentication. This system solves the problem of remembering alphanumeric or several click-points by replacing multiple image sequence with a single window containing a one set of images.

The visual representation of 4 sets of graphical image authentication will be given to user, in which the first three set contains several words. And the 4th set contains set of images. User can choose any one of the four sets . All the sets are in form of 4x8 matrix . Since the window frame contains 128 images it is completely impossible for the attackers to guess the sequence of click-points on the images. Additionally the proposed work introduces a secret key technique that improves the remembrance of the password. Also includes shuffling the sequence of images contained in the window frame. The proposed system figure 2 performs well in terms of security, accuracy and ease of use.

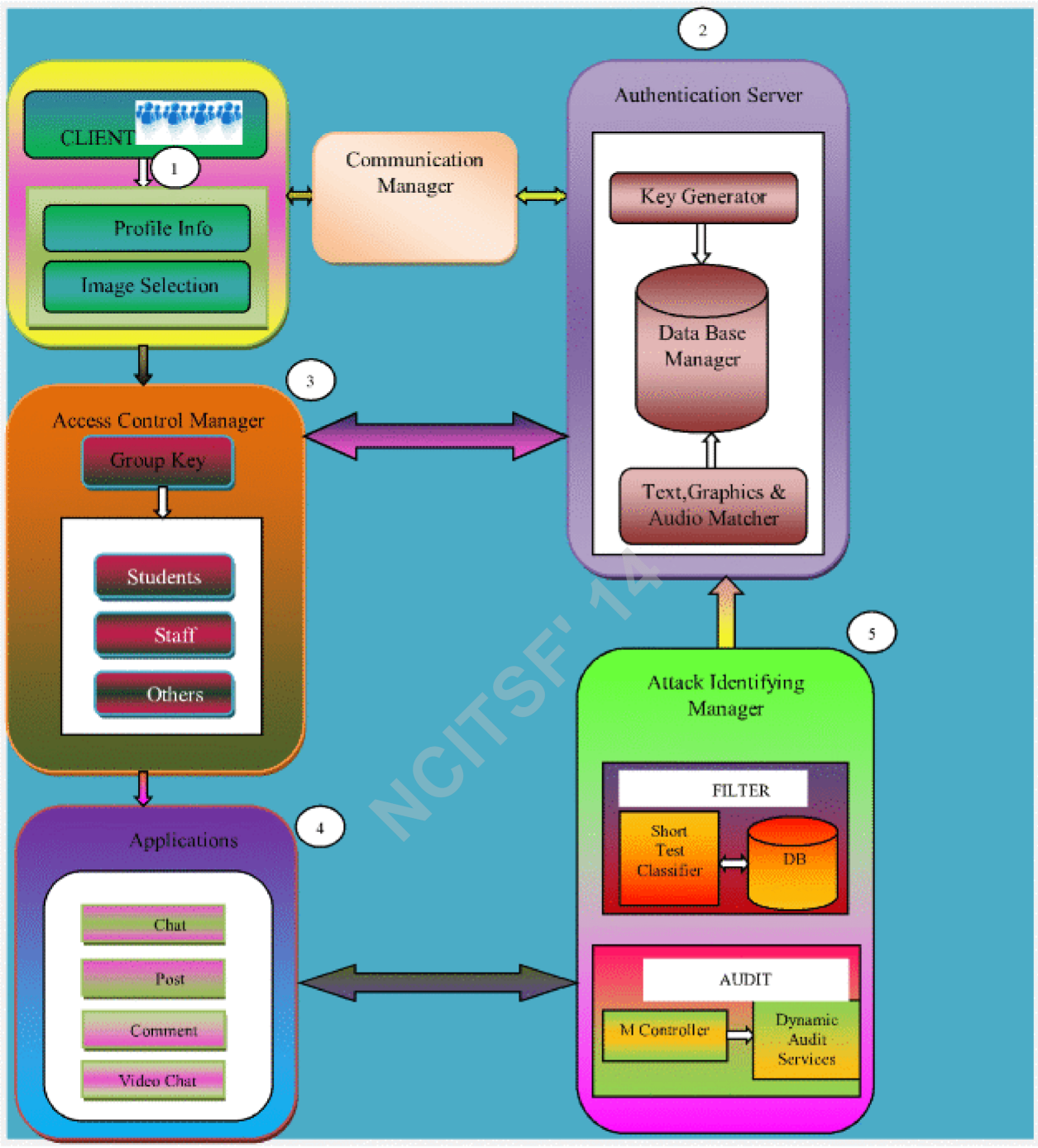
VII. FUNCTIONALITIES OF PROPOSED FRAMEWORK

The various functionalities of the framework are well presented in below.

CLIENT REQUESTER (CR) – The Client Requester is a user (i.e. student, staff, others) of OSNs. The client has made a request to AS for registration in proposed OSN. The Authentication server also allows the clients for registration over the internet. Once the registration process is completed, the Authentication server generates a unique key for the client and save all the client details in the Data Base Manager. During login the client provides correct answers

for the security authentication in order to get the unique key to access any applications in the server.

COMMUNICATION MANAGER (CM) – The Communication Manager (CM) acts as a communication medium between the client and server. It transfers the communicates the client request to the server and server response to the client. It acts as an intermediate between client and server. The requester interfaces are secured using Public Key Infrastructure mechanism.



AUTHENTICATION SERVER (AS) – The Authentication Server (AS) keeps a record of all registered clients. The authentication of the client is done by the authentication server by matching the images in proper order with the order of the images stored in the Data Base. After authentication, AS establishes connection with Data Base Manager for retrieving user's details, The information flow on the network is secure by encrypting and decrypting the message using RSA algorithm. The Authentication Server setup consists of a Key Generator, Image Matcher and Data Base Manager.

KEY GENERATOR (KG) – The Key Generator (KG) generates a unique key for every client once the authentication is given to the user. It stores the unique key in the Data Base Manager inside the server. The key is encrypted using RSA algorithm for security reasons.

DATA BASE MANAGER (DBM) – The Data Base Manager (DBM) stores all the client details along with their security unique key. The profile info of every user is stored in the database. It contains Image Matcher (a set of images) for verification of Graphical image authentication. All data inside the Data Base Manager is in encrypted form.

IMAGE MATCHER (IM) – The Image Matcher (IM) verifies the Graphical image authentication. It matches the image order selected by the client to the image order stored in the Data Base.

If the order matches, it indicates to the server to give authentication to the client else server displays an error message to the client. The images inside the IM are stored in encrypted form.

AUDIO MATCHER (AM) – The Audio Matcher (AM) verifies the audio file authentication. It matches the image order selected by the client to the audio order stored in the Data Base. If the order matches, it indicates to the server to give authentication to the client else server displays an error message to the client. The audio inside the AM are stored in encrypted form.

VIII. IMPLEMENTATION

8.1 Implementation module

The implementation has mainly three modules: New user registration, Existing user Login and Recovering Password.

A . New user registration:

Registration phase

In this phase, the client requester is authenticated by registering oneself in the authentication server. At the time of registration, the user provides his personal data such as name, email, address, gender, birth date, login etc. Email entered by the user will be validated and if it is a invalid email, user will get error message. Also user needs to answer a set of security authentication (Questions for security verification). 4 sets of graphical image authentication will be given to user, in which the first two set contains several words split into different cells. And the , 3rd set contains color image, and 4th set contains set of object images. User can choose any one of the four sets. If the user chooses the any one of the first 3 sets, user need to

drag the words from various sentences and place it in the given box. The arrangement of words will be the password. If the user chooses 4th set of graphical authentication, user needs to arrange a set of random images in an order to create password. After choosing the graphical image, choose the audio file After completing the registration, the user will be able to login to the website by entering login id , Graphical image and audio files authentication (i.e. arranging the set of random images in the same order ,which user arranged during the time of registration). Then the user will be able to login to their profile page. Thus secure registration is provided using this phase. The following Fig.3 shows registration phase.

Key generation phase

In this phase, a Graphical User Key is generated during the registration phase which needs to be arranged by the user in any order. Once the registration is completed a unique key is generated for each user. And whenever the user tries to login to the website the Graphical image authentication is displayed in random order every time and the user needs to arrange the images in the same order which they arranged during registration. Once the user login to the website, in order to use any features in the website such as uploading/downloading photos, chatting with friends etc. User needs to answer a set of security authentication which was answered during registration phase, If the answers are correct, key generator generates the unique key immediately to access the features in the Framework.

B. Existing user Login:

If the username and password is correct the server authenticates the user to access the website else displays a

error message. Once the users log in to the website, in order to access any features they need a unique key. In order to get the unique key, users needs to click "find key" link, once the link is clicked it will display the set of security authentication which was answered during the registration. If the answers are correct, AS authenticates the user and provides the unique key else displays a error message. After getting the unique key, the user will be able to use the features such as chat, video chat, post etc in the proposed framework. Existing users should give userID and enter secret key.

C. Recovering Password:

If the username and password is entered incorrectly for more than 3 times. The user could retrieve password (the sequence of selected six images) by using the security question that he entered during the registration process. The user retrieve password by getting the current shuffled picture.

Figure 3: Registration Phase

IX. SCOPE AND SIGNIFICANCE OF STUDY:

There is an ample scope of research in the stated area. Present study will reflect the importance of security in network and will provides the better encryption technique for currently implemented encryption techniques. It will explore how to tackle with the threats to data integrity and for safe passage of data from one node to another. This research will provides the great feasibility for authentication process improvement for security in network.

IX. COMPARISION

Parameters	Plane Network	RSAand MD5
Application Response time	15	12
Load	1650 seconds	1400bits sec
Throughput	7000bits sec	3750bits sec

X. CONCLUSION

In this paper, we discuss an efficient and secure hybrid algorithm for providing security to social network nodes. Since we have tested our proposed algorithm with different scenarios and it is providing better response time, less network delay and best throughput. These parameters have been shown in above table. We got better results than other algorithms so proposed algorithm can be implemented to social network nodes for security purposes. Also our research shows that it is helping in efficient routing of packet with much less load on servers

REFERENCES

[1] Tsai, D.T., A.Y. Chang, , S. Chung, Y.S. Li, "A Proxy based Real-time Protection Mechanism for Social Networking Sites," in Proc. ICCST 2010.

[2] Graffi, K., P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, R. Steinmetz, "Practical Security in P2P-based Social Networks," in Proc. IEEE 34th Conf. on Local Computer Networks, pp. 269-272, 2009.

[3] Durr, M., M. Werner, M. Maier "Re-Socializing Online Social Networks," in Proc. GREENCOM-CPSCOM'10, pp.786- 791, 2010

[4] Hogg, T., "Security Challenges for Reputation Mechanisms using Online Social Networks," in Proc. AISec'09, pp. 31 –34, 2009.

[5] Shin, D., R. Lopes, W. Claycomb, G. Ahn, "A Framework for Enabling User-Controlled Persona in Online Social Networks," in Proc. of the 33rd Annu. IEEE International conf. on Computer Software and Applications, pp. 292–297, 2009.

[6] Ho, A., A. Maiga, E. Aïmeur "Privacy Protection Issues in Social Networking Sites" in proc. AICCSA , pp. 271-278, 2009.

[7] Diaz-Sanchez, D., A. Marin, F. Almenarez, A. Cortés, "Social Applications in the Home Network," in proc. of the IEEE Transactions on Consumer Electronics, Vol. 56, No.1, pp. 220–225, 2011.

[8] Anderson, J., C. Diaz, J. Bonneau, F. Stajano, "Privacy-Enabling Social Networking Over Untrusted Networks," in Proc. WOSN'09, 2009.

[9] Beach, A., M. Gartrell, R. Han "Solutions to Security and Privacy Issues in Mobile Social Networking," in Proc. International Conf. on Computational, 2011

[10] Matthew Wright, Apu Kapadia, Mohan Kumar, and Apurv Dhadphale, "Reputation for Directory Services in P2P Systems" in Proc. CSIIRW '10, pp. 21–23, 2010.

[11] Carminati, B., E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thurain singham, "A Semantic Web Based Framework for Social Network Access Control" in Proc. SACMAT'09, pp. 177-186, 2009.