EFFICIENT AND SECURED TECHNIQUE FOR AUTHENTICATION OF SOCIAL NETWORKING SITES

MUHAMMED Sanusi[1], CHUKWUDOZIE Ndidiamaka[2], MUSAH Abdulmumini Yakubu[3]
Senior Lecturer[1], Research Scholar[2-3]
[1-3]Computer Science Department, University of Abuja,
Abuja-Nigeria.

ABSTRACT

Social Networking sites are generally vulnerable to insecurity and this causes the risk of attack and leaking of personal information by unauthorized and unintended recipient users. The contemporary web services provide users with an alternative email address or security question to recover passwords for their page. However, this approach can easily be broken by other unauthorized users. In this research work, a more efficient technique using two-layer phases is proposed. The technique involves; (i) Backup of personal details. (ii)The use of trusted friends to recover the password. The trusted friends are configured in the initial registration of the user. This paper reviewed other research work that was conducted in the area. In the research, the use of encryption is considered to be adopted and a blowfish algorithm is found to be better and more secure.

KEYWORDS: *Social Networking Sites, Security, Encryption.*

1.0 INTRODUCTION

Social Networking sites nowadays use passwords to authenticate users. But there are certain problems with this: the user may forget his password or the account may be hacked by the attacker. This authentication mechanism is insecure and unreliable. Authentication is a mechanism in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. Social networking sites have become popular in recent times. However, in traditional authentication mechanism password, fingerprint, security questions are used. However, password-based authentication didn't provide strong security for the system with sensitive data. Many attackers are still able to overcome these security countermeasures by different techniques. Currently used authentication mechanism security question is easily guessable and phished by the attackers.

Social media had been compromised from the security perspectives thereby posing a great threat to users concerning their personal, intellectual, career property. The security threats range from privacy setting threats, identity-related attacks, social attacks, anonymity attacks, and information leakage attacks. Though some of these threats can be combed by simply enlightening the users on potential threats. For instance, a survey reveals that 25% of Facebook users don’t bother with privacy settings[1].

The main purpose of this research is the security and reliability of authentication of social networking sites in which previous work does not show the mechanism of safely data dissemination from one user to another. As there are various security issues in existing social authentication and user data privacy is compromised.

2.0 LITERATURE REVIEW

Security threats mitigating the efficiency of Social networking sites can be categorized into three groups: (i) Confidentiality of data. (ii) Integrity of data (iii) Availability of service.

Companies have suffered loss in aspects such as financial information leakage, and network resource wastage due to unreliable and inefficient security[2]. The table below illustrates several numbers.

TABLE 2.1: Review of Related Literature of work that has been achieved in the area of social networking sites.

S/N	Author(year)	Title	Aim/Objective	Motivation	Methodology(ies)	Result	Limitation(s)
1	(Sagar & Waghmare, 2016) [3]	The Security and reliability of Authentication of Social Networking Sites	to detect attackers and try to optimize the number of attacks, and do safely data dissemination from one user to another user without data missing and with using a high-security process	Insecure and unreliable password recovery	The use of multifactor authentication process	No attack is known to be successful against it	The application must be tested over a network
2	(Obiniyi, Oyelade, & Obiniyi, 2014) [4]	Social Network and Security Issues: Mitigating Threat through Reliable Security Model	Ensuring user authentication, sustaining confidentiality and integrity of information in Social networking sites	Increasing growth of users of social networking sites and more vulnerabilities to attackers	Show the security measure to ensure information confidentiality and integrity between users of a social network with a model	The use of a hash function and cryptographic model against attacker was successful	The application must be tested over a network
3	(Polakis et al., 2014) [2]	Security and Privacy Measurements in Social Networks: Experiences and Lessons Learned	Presentation of experiences from research on Facebook	The scale nature of online social networks services requiring efficiency and accuracy	The use of photo base social authentication	The experiment shows that an attacker can obtain access to sensitive information for at least 42% of a user’s friends that facebook uses	Interacting with a large – scale social networking site like Facebook, to conduct a user-centered analysis

Social media had been compromised from the security perspectives thereby posing a great threat to users concerning their personal, intellectual, career property [5]. These security threats range from privacy setting threats, identity-related attacks, social attacks, anonymity attacks, and information leakage attacks.

It is imperative that social networking uses encryption to further secure communication. Table 2 summarizes several encryption techniques adopted.

Table 2.2: summarize several use encryption and their challenges.

Encryption Type	Features	Challenges
AES (advanced encryption standard) is a symmetric encryption algorithm and one of the most secure [6].	Security: Competing algorithm where to be judged on the ability to resist attack. Cost: Intended to be released under a global, non-exclusive and royalty-free basis, the candidate algorithm where to be evaluated on computational and memory efficiency. Implementation;	Research into attacks on AES encryption has continued since the standard was finalized in 2000. Various researchers have published attack against reduced-round versions of the advanced encryption standard
3DES (triple data encryption standard) is a current standard and a block cipher [7]	Officially, the 3DES algorithm (TDEA or Triple DEA) is a symmetric key block cipher algorithm three times to each data block	3DES were a series of brute force attack contest created by RAS security to highlight the lack of security provided by DES.

This research has identified blowfish encryption algorithm will better suit social network sites communications can be used as a replacement for DES or IDEA algorithm. It is asymmetric (that is a secret or private key) block cipher that uses a variable-length key making it useful for both domestic and exportable use.

Symmetrical Encryption

Also known as secret-key encryption, symmetrical cryptosystems require the sender and receiver to have the same secret key [8]. This single key is required for both the encryption and decryption of the message.

Asymmetrical Encryption

Asymmetrical encryption methods also referred to as Public Key encryption systems were developed in 1976 by Whitefield D. and Martin H. [9]. The principle of public-key encryption is that both parties, the sender as well as receiver, have a pair of keys. The one key does not have to be kept secret and is called the public key. The two different keys held by the parties have different uses; one is used for encryption and the other for decryption. The encryption key is the "public" key, while the decryption key is the "private" key. The private key must be kept secret.

3.0 AUTHENTICATION METHODS

How someone may be authenticated fall into three categories, based on what is known as the factors of authentication [10]. Each authentication factor covers a range of elements used to authenticate or verify a person's identity before being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified. The three factors and some of the elements of each factor are:

- **The Knowledge Factors**: Something the user knows (e.g., a password, partial password, passphrase, or personal identification number (PIN), challenge-response (the user must answer a question or pattern), Security question. Password Authentication Protocol is such a method for knowledge factor.
- **The Ownership Factors:** Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token). Authentication Token is such a method for ownership factor.
- **The Inherence Factors:** Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier). Bio-metric Authentication is such a method for the inherence factor.

4.0 METHODOLOGY

The proposed share portal system will have a login system that will ensure that the authentication of the right user is safe and secure using the "BlowFish" encryption algorithm implemented in PHP (Personal Home Page Hypertext Programming) language. Blowfish is an encryption algorithm that uses a variable-length key from a 64-bit block cipher. The proposed system in the system design evaluated using PHP.

The user interface (UX-User Experience) at the frontend of the proposed system will be developed with Twitter bootstrap technology comprising of HTML (Hypertext Markup Language), CSS (Cascading Style Sheet), and JQuery framework of javascript.

The MySQL Relational database system will be incorporated into the system for the storage of the user's login credentials and authentication at the backend of the application.

The tools will be used for project development:

- Sublime Text 3: The text editor for the coding and debugging of the software application program.
- WampServer: The Windows, Apache and MySQL, PHP server software that the proposed application will be developed on.
- Development Platform: A windows 10 Operating Systems Computer with at least a 2Gigabyte of RAM, and 320 Gigabyte of magnetic Hard disk storage.

5.0 SYSTEM DESIGN PROCEDURES

The system is designed in such a way that any organization can use the application to share files among themselves and it is customizable. The application is made up of two areas: the public area and the admin area

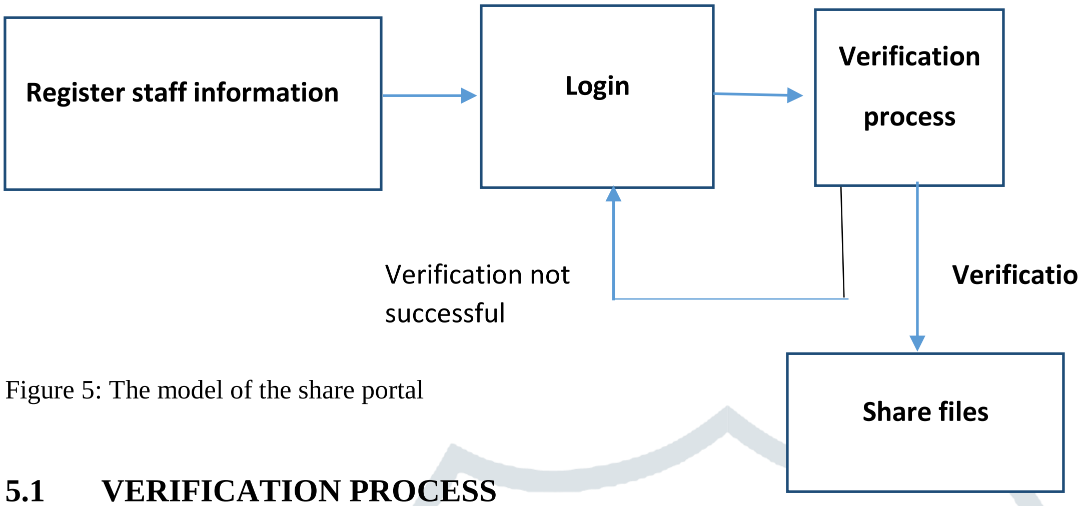

Figure 5: The model of the share portal

5.1 VERIFICATION PROCESS

The user will first sign up to the application as a member with his or her surname, middle name, Lastname, department, email address for verification, secret password to log in. When the submission is successful, the staff can now login with the three names and the passwords submitted, and get an OTP (One time password) random generated numbers into his or her email registered with for the authentication process to give him or her access to the main staff page where files and information are shared in the organization.

5.2 ADVANTAGE OF VERIFICATION OVER EXISTING SYSTEM

The existing system of verification generates personal questions of the individual for answers like what is your pet animal, what food do you like most. A hacker can predict the right answers to these questions if they know the victim's personal life or understudy them. But the proposed system generated only random number of variable lengths to the user which make it difficult for the attacker to predict, this is why most financial institution use this method for payment transactions on the internet.

6.0 CONCLUSION

In this research work, a two-layer security measure technique is proposed (i) the user login authentication phase and (ii) the one-time password code email validation phase. This method will allow a better-secured technique against attackers or spying. It is difficult for unauthorized users to guess the login credential of the original user. The adoption of blowfish encryption is also found to be more suitable after reviewing all relevant literature.

REFERENCES

1. Zhang, Z. and B.B. Gupta, *Social media security and trustworthiness: overview and new direction.* Future Generation Computer Systems, 2018. **86**: p. 914-925.
2. Polakis, I., et al. *Security and privacy measurements in social networks: experiences and lessons learned*. in *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. 2014. IEEE.
3. Sagar, K. and V. Waghmare, *Measuring the Security and Reliability of Authentication of Social Networking Sites.* Procedia Computer Science, 2016. **79**: p. 668-674.
4. Obiniyi, A., O. Oyelade, and P. Obiniyi, *Social network and security issues: Mitigating threat through reliable security model.* International Journal of Computer Applications, 2014. **103**(9).
5. Sánchez Abril, P., A. Levin, and A. Del Riego, *Blurred Boundaries: Social media privacy and the twenty-first-century employee.* American Business Law Journal, 2012. **49**(1): p. 63-124.
6. Singh, G., *A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security.* International Journal of Computer Applications, 2013. **67**(19).
7. Alanazi, H., et al., *New comparative study between DES, 3DES, and AES within nine factors.* arXiv preprint arXiv:1003.4085, 2010.

8. Garg, P. and J.S. Dilawari, *A Review Paper on Cryptography and Significance of Key Length.* International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering," ICE TIE, 2012.

9. Morkel, T. and J. Eloff, *Encryption techniques: a timeline approach.* Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, 2004. **2**.

10. Smith, L., I. MacDonald, and A. Zeltser, *Authentication factors with public-key infrastructure*. 2009, Google Patents.