ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Accessing Distributed System Using Hashed Fingerprint Recognition

R.Mekala[1], S.A.Jiji Jasmine[2], Vinisha.D[3]

M.E, Communication Systems, Department of ECE, SNS College of Technology, Coimbatore, Tamil Nadu, India[1, 2, 3]

ABSTRACT-The security threats to personal information are the major problem which resists from providing a secured access to users. A user may have a large number of web accounts and will find difficult to remember their password for all accounts which raised uniqueness in password. However, there are some secure services that revolve around the distributed sharing of data, and do not provide a high level of security for signing into accounts. This paper presents remedial measure for having a high level of security, named hashed fingerprint which is wiser in providing secure access of web accounts on comparing with already existing methods. Here we use AES and SHA-1 for encrypting the fingerprint that is obtained as the password.

KEYWORDS: Secure, AES, SHA

I. INTRODUCTION

Network security starts with authenticating the user commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone) and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).

Cryptography is a concept to protect our network and data transmission over wireless network. But also in cryptography it uses various types of encryption algorithms to change the plain text to cipher text. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security.

The main factor in choosing encrypting algorithm is that it should resist collision attacks also it should have less processing time for encrypting the plain text and also it should be very tedious task for the hackers which should take a long years to retrieve the original during hacking. Also hashing technique plays a major in our paper which deals in encrypting the plain text for the second time. Thus we use two stages of encrypting the text which is known as cipher after encrypting with AES and known to be message digest after encrypting with hash function SHA-1. Thus only after encrypting with hash function we use the digest as password for distributed system which we going to implement on company domain [8].

II. EXISTING METHOD

From the survey carried out, regarding the number of accounts held by internet users about 44% of the users have more than 15 web accounts. So, the user will face great difficulty in remembering their log-in details and passwords. FingerID is a common practice to give away differing information on web It provides service of filling out the registration forms by giving the respective service provider with user's credentials. FingerID comprises of Four-Tier architecture. They include Client, Interface, Control and Distribution [16].

Hash Functions

There are two primarily cryptographic hash functions in use today, MD5 and SHA1 [1]. MD5 stands for "Message Digest 5" because it is the fifth revision of a message digest algorithm devised by R.L. Rivest of RSA Laboratories (RSA Laboratories). The early revisions of this algorithm were published prior to 1989, and the most recent revision of the algorithm was published in 1991. It has an arbitrary input length and produces a 128-bit digest (Rivest). Although weaknesses have been found in the algorithm, there has never been a published collision.

SHA1 stands for "Secure Hash Algorithm 1", it is the first revision of a hash algorithm developed by the National Security Agency. The algorithm was first published in 1995 (Wikipedia). SHA1 supports messages of any length less than 264 bits as input, and produces a 160-bit digest. In the unlikely event that one wishes to compute the digest of a message larger than 264 bits in length (over 2 billion GB of information), the simplest solution would be to divide the large messages into smaller messages. There are no known weaknesses in SHA1, and it is generally considered the more secure of the two algorithms. There are also variations of SHA1 which produce longer digests, SHA-256, SHA-512 [10]. They produce digests of 256 bits and 512 bits, respectively (Eastlake).

The SHA1 and MD5 algorithms are considered secure because there are noknown techniques to find collisions, except via brute force. In a brute force attack random inputs are tried, storing the results until a collision is found. If we do not limit ourselves to finding a collision with a specific message, one can expect to find a collision within 2n/2 computations, where n is the number of bits in the digest. This means that an attacker would need to compute the digests of approximately 264 messages to find a collision in the MD5 function, and approximately 280 computations to find a collision in SHA1. Note that SHA1 may be more secure than MD5, but it is more costly to compute a message digest using SHA1 than MD5. If one is expressing security concerns SHA1would be the function of choice, however, if speed is an issue it is likely that MD5 would result in faster performance, and would likely still be secure enough for most applications. They also use register algorithm and various encryption algorithm for their experiments.

III. PROPOSED METHOD

In our experiment we going to combine the encryption and hashing techniques together to prove a high level of security. The encryption using AES is done for the fingerprint that is entered through the fingerprint scanner interface [6].In this paper we develop E-mail System for domain creation communicate to user and by send or receiving e-mails using Human finger print as password for better security. User finger image is further encrypted using encryption algorithms before storing into data base for better security [5].

Fingerprint identification has a number of advantages which make it a popular method of identification in settings ranging from police stations to secured facilities [16]. This method of identification is accomplished by comparing fingerprints from someone against a database of known fingerprints. If the sample fingerprints match fingerprints in the database, it is considered a positive match. It is important to note that many identification systems which use fingerprints go for a statistically significant match; rather than matching the whole fingerprint, they look for key markers which can be used for comparison.

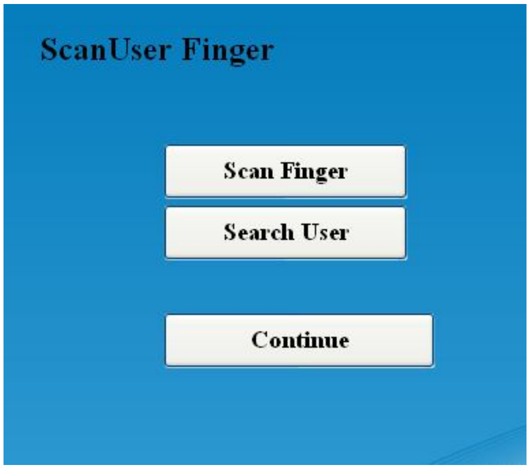
Authentication is typically used in circumstances where access is being controlled, whether physical access to a room or building, or access to an electronic system such as the logon to a computer system. Biometric authentication thus processes a one-to-one match rather than a one-to-many search [3]. For both the identification and the authentication systems, a threshold will generally be used to determine the match between templates.Many systems have been developed for implementing biometric identification and authentication.Even for a single biometric, such as the fingerprint, there are many different methods used to create the biometric template.

MODULES USED

The login using finger is for getting scanned input of fingerprint with the help of interface kit. After getting the input its encrypted first with AES algorithm and then again encrypted text is further hashed using hashing algorithm (SHA1) [10]. To obtain the input and for encryption we use the programming language ASP.NET. Now the encrypted text is stored in the database for which we use SQL language. The domain creation is done by the administrator by using ASP.NET. The rights for the domain group user is been egresses by the administrator of the domain.

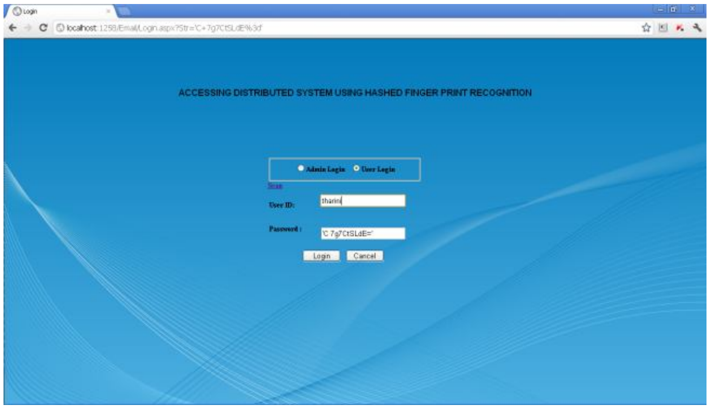
1. Login using finger print

The user simply places their finger on the glowing reader window, and the reader quickly and automatically scans the fingerprint. On-board electronics calibrate the reader and encrypt the scanned data before sending it over the USB interface.If the user is existing ,they can access using registered username and password by scanning their finger print, otherwise user have to create new account.



2. Encrypt user finger and store to database

The scanned finger print from the user is encrypted using AES algorithm by converting into digital data and stored in the database(As back end using sequential query language).


localhost:1258/Email/Login.aspx?Str='C+7g7CtSLdE%3d'

ACCESSING DISTRIBUTED SYSTEM USING HASHED FINGER PRINT RECOGNITION

○ Admin Login ● User Login

User ID: tharini

Password : 'C 7g7CtSLdE='

There are three basic classes of AES cryptographic algorithm:

• To encrypt relatively short messages

• To compute digital signatures

• To establish or verify cryptographic keying material.After scanning the finger image of the user is further encrypted by using encryption algorithm and it is stored in the database.

3. E-mail domain creation

A domain name is the name to identify a website. Having your own domain nameand redirecting it will make sure that your prospects end up in the right place and you don't lose their business. An administrator creates and monitors the domain. Total number of users should be declared while creating the domain.

4. User creation and providing rights

Creating users is a significant application of E-mail domain. Modifications made in the user accounts will automatically get updated in its database.Administrator of this domain assigns rights to the user for accessing their accounts.

5. Send and receive data using fingerprint login

Only registered users are allowed to communicate within that domain based on the rights provided by the administrator.

IV. CONCLUSION AND RESULT

Our experimental result has an extensive study of existing applications and relevant literature enabled understanding the requirements of accessing the web accounts with security, accessibility and usability. FingerID is a proficient and trustworthy alternate to the conventional authentication mechanism of username and password. FingerID has been developed with an objective of improving the process of log-in in the user's web accounts.

Comparison of various authentication mechanisms is shown below:

Current application	Level of security	Level of accessibility	Level of usability
Open ID	Yes	No	No
Shibboleth	Yes	No	No
OAuth	Yes	No	Yes
Liberty Alliance	No	No	Yes
Microsoft passport	No	Yes	Yes
FingerID	Yes	Yes	Yes

Username and password are usually kept simple which help the intruders to hack the password easily and also another important thing is that user may keep same password for multiple accounts which enables the intruders to hack more information about the user. FingerID will enhance the security to user account in all aspects which will have greater convenience to everyone. Also in our paper we have given two stages of security where first is done by encrypting the given fingerID by AES algorithm and second stage by encrypting the AES cipher with hash function which will provide a high level of robustness to users.

The findings of this paper will revolutionize the entire authentication mechanism on the web, and thereby enable the user access to distributed accounts at a single point. FingerID will authenticate the user on the basis of his fingerprint scans. Other biometric authentication methods—for example, palm prints and face gestures—will be taken as a goal for the future. Another aim of the project is to encourage further research and development on the subject.

REFERENCES

[1] AmandeepKaur,AmandeepVerma, "Cryptography and its hash function's security".

[2]Carlos Cid, "Recent developments in cryptographic hash functions: Security implications and future directions"

[3]D. Chou, "Strong User Authentication on the Web", Microsoft Corporation, August 2008.

[4] FIPS pub 198, "The Keyed-Hashed Message Authentication Code", March 6 2002

[5] G. J. Popek, C. S. Kline, "Encryption and secure computer networks", ACM Computing Summit.

[6] IsmetOzturk and ImbrahimSogukpmar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology, 2005.

[7] L. K. Hoa, T. X. Phuong, "Distributed Systems Security", *Technical Report*, 2009.

[8] J.Dollimore, T. Kindberg, "Distributed systems: concepts and design", Addison Wesley/Pearson Education June 2005.

[9] J. Jackson, "OAuth 2.0 security used by Facebook, others called weak", Computerworld Security newsletter, IDG.net, 2010.

[10] John Edward Silva, "An Overview of Cryptographic Hash Functions and Their Uses", SANS Institute, 2003.

[11]M. Engel, "MySpaceID Usability Testing", Slide Share.net, MySpace, 2009.

[12] M. McGinity, "Staying connected: Let your fingers do the talking", Communications of the ACM, vol. 48, no. 1, 2005, pp 21-23.

[13]M. Soshi, M. Maekawa, "The Saga Security System: A Security Architecture for Open Distributed Systems", IEEE, 1997

[14] Muxiang Zhang, "New Approaches to Password Authentication Key Exchange Based on RSA", Verizon Communication, Inc, August 18, 2004.

[15]M. V. Ramakrishnan, Justin Zobel "Performance in Practice of String Hashing Functions, RMIT.

[16] Sara JezaAlotaibi, Mike Wald, David Argles,"Using Fingerprint Recognition in a New Security Model for Accessing Distributed Systems",IJICR.

[17] T. DiVito, "OpenID: A Potential Authentication Technology", Decision Line, School of Business-Camden, Rutgers University, New York, USA, 2008.