Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Authentication Mechanisms For Signature Based Cryptography By Using Hierarchical Scheme.

K.K.Priya[1], M.Mailsamy[2] and B.M.Brinda[3].
[1] *Dept of IT, Vivekanandha College of Engineering for Women*
[2]*Dept of IT, Vivekanandha College of Engineering for Women*
[3]*Dept of IT, Vivekanandha College of Engineering for Women*

Abstract— In this paper the signature of a person is taken as input which is encrypted using hierarchical visual cryptography. By using HVC the input signature will be divided into four shares. From that any three are taken to generate key share. Another fragmentation should handover to the authenticated server. The authenticated server should maintain the generated key and fourth fragmentation. Only the authorized user can be accessed. If the receiver identifies the fourth fragmentation and decrypt they got message by using HVC. It is insecure process because anybody can hack the decrypted message easily. For the secure process the authenticated server generate a password while transferring a message. The authenticated person can only able to got that message. The authenticated server checks whether the person should be authorized user or not, while starting their conversation. It provides more security and challenged for the hackers.

Keywords- Hierarchical visual cryptography, Secret sharing, Authentication server, Fragmentation, Security analysis.

I. INTRODUCTION

Network is a group of two or more computer systems linked together. It can interconnect with other networks and contain Sub networks. Computer Network is a telecommunications that allows computer to exchange data. The computing device pass data to each other along data connections or network lines between nodes are established using either cable media or wireless media. The best known computer network is the Internet.

Network Security concerned with protection of data from unauthorized access. In a typical network environment there are three aspects of information of security such as, Security Attacks, Security Mechanisms, and Security Services. Security attacks: Actions which compromise the security of information. Security Mechanisms: It is a method to detect, prevent, or recover from security attacks. Security services: A service which employs one or more security mechanisms to enhance the security of the network. The security mechanisms contain Confidentiality, Authentication, Integrity, No Repudiation, Access control, Availability. A host can be a server, a workstation, or a device such as a router. Any system or device connected to a network is called Host.

The concept of hierarchical visual cryptography is based upon visual cryptography. Visual cryptography encrypts the informative image into two shares so that one cannot reveal the original information in absence of other. To decrypt the secret, both shares are required to be super imposed with each other. The original secret is divided into exactly two shares. Hierarchical visual cryptography can encrypts the secret in the form of levels. Initially the secret is encrypted to generate two shares. Later these two shares are encrypted independently generating four resultant shares. Finally any three shares are collected to generate the key share. The server has special software called host refers to any computers or device that is connected to a network and sends or receives information on that network. A host can be a server, a workstation, or a device such as a router. Any system or device connected to a network is called Host. The host is used for sending and receiving the nodes by the authenticated server.

HVC mainly used to secure the data from unauthorized users in data security. It secures the network as well as protecting and overseeing operations being done in HVC. It is a series of points or nodes interconnected by communication paths. Many authentication systems are proposed which is based on fingerprint and Iris. These authentication mechanisms are mainly used in Army and banking, etc for the human identification and security. The signature is a special pattern provided for human authentication at the security level. It is great importance and more reliable for the stated mechanism in HVC. By using HVC it provides more security and challenged for hackers. The key share generated is having random techniques.

II. RELATED WORK

The concept of Secure Iris Authentication is done by visual cryptography. The system uses the human eye iris for authenticate purposes. Before storing the iris in central database, it is encrypted using visual cryptography scheme. Visual cryptography provides extra layer of authentication in the system. In the system enrolled iris template is divided into two shares using visual cryptography, one is kept in the database and other is placed on the user ID card. Iris template is secured by using only one share by the database in which no information can be retrieved for the enrolled eye image. Thus the unauthorized user is prevented [1]. By using the intelligent system the security of the authentication is secured. In the visual cryptography the secret sharing is done by dividing the secret information into number of parts. Since it shares individual information, it is unable to reflect secrecy of the data. Hence in future the security in multiple levels can be improved. [2]. Diffie-Hellman key agreement protocol and visual cryptography scheme were merged for the discovery of the new cryptographic scheme. The newly implemented scheme verifies the shadows which are authentic before reconstructing the secret image. Then it was found to be secured than plane visual cryptographic scheme because it has low computations in authentication [3].

Yi Hui Chen and Pei Yu Lin proposed a novel secret sharing scheme using low computations for authentication. The advantage in the scheme is the pixel expansion which has 1:1 ratio. The secret sharing can be modified without any loss of information. Since it cannot authenticated with the half secret key which is infeasible for signature based authentication. By using the Boolean operations the secret key can be encrypted [4]. Image Captcha Based Authentication Using Visual Cryptography Preserve the privacy of image by degenerating the original image by using Blowfish algorithm, Splitting & Rotating algorithm. It attack globally and capture and store the user's confidential information. The image Captcha is readable by human users alone and not by machine users [5].

The hierarchical visual cryptography provides expansion less shared key. The encrypted secret key in various levels is done by designing and the implementation of hierarchical visual cryptography. The encryption in turn is expansion less by using Greying Effect (GE). The expansion of secret key takes place after encryption, which reflects some GE. The GE is completely removed while revealing the secret removal of GE [6]. The efficient delegation of key generation and revocation functionalities is used in Identity-Based Encryption (IBE). The efficient solution of the revocation or delegation of key generation is done by using IBE. When a secret key is corrupted by hacking the period of a contract is expires. Thus it reduces the excessive workload for a single key generation authority [7]. Attribute-Based Encryption (ABE) is the hierarchical access structure. The public keys allow encrypting an unbounded number of users by using ABE. The key storage is significantly more efficient than all solutions. Encrypt key size without compromising on other critical parameters [8].

III. EXISTING WORK

HVC divides input signature into four resultant shares. Among four shares, any three are taken to generate key share. Remaining share is handed over to the user and the key share is placed on authentication system. If the receiver identifies the fourth fragmentation and decrypt they got message by using HCV. It is insecure process because anybody can hack the decrypted message easily. The Signature is the most common authentic entity from the user side which has been used earlier in various confidential purposes. For improving security of authentication system, the signature is required to be enrolled and verified.

It Change the pixel distribution of the image when unauthorized access is going on by using Fool-Proof Lock-Key, Sub pixel Keys can be duplicated easily even without using the original key. Every lock-key pair has one associated unique image. It cannot be duplicated. Automatically preserve the privacy of captcha by using Anti-phishing methodology. The Attackers use such information for monetary benefits for secure and prevent the phishing attacks.. When a secret key is corrupted by hacking or the period of a contract expires. Reduce excessive workload for a single key generation authority. The public key allows encrypting an unbounded number of users by using Attribute-Based Encryption. Key storage is significantly more efficient than all solutions. Encrypt key size without compromising on other critical parameters.

The simple share is the part of database in the system. As the database of the entire authentication system includes the scrambled form of the share, there exist least possibility of various attacks like dictionary attack and bruit force attack. During authentication, employee should insert the smart card in the card reader mounted in the entrance card. If the card is stolen in that case it will not be of any use to the unauthorized user but authorized user will be issued a new card. It generate the key share randomly techniques.

A. Methodology for Hierarchical Visual Cryptography

Hierarchical visual cryptography is defined on basis of visual cryptography. Simple visual cryptography divides original secret in two parts. Each part is known as share. To reconstruct the secret, both shares are stacked together. Hierarchical visual cryptography also encrypts the secret information in two shares at the first stage. Later, these two shares are encrypted individually to generate subsequent shares.

The second level of hierarchy in HVC is found the four resultant shares Out of these four shares, any three shares are taken to generate the key share. This stage is identified as third level of HVC. Finally, HVC scheme gives two resultant shares out of which one is handed over to the user for authentication and another share is along with database. Original secret is an input to the system. Two shares are generated out of expansion less visual cryptography module. These two shares are independently encrypted. Key share generator module is responsible for generation of key share. Key share is combination of first three shares taken from previous level of hierarchy. Here *A* indicates key share and *B* indicates remaining share. Percentage of black and white pixels remains constant for different category of secrets like images, handwritten text and textual passwords. It has been analyzed that the concentration of white pixels decreases drastically in first level of hierarchical visual cryptography. This concentration remains steady for second level and later increases at the end of hierarchy. Key share reflects high concentration of black pixels. The revealed secret represents high concentration of white pixels.

IV. PROPOSED WORK

Hierarchical visual cryptography increases the security by encrypting the signature. The card reader reads the key share from card and superimposes over the corresponding simple share available in the database. For verification of an employee, revealed signature is matched with enrollment number. In this authentication system, unauthorized user can not authenticate. It encrypts the input secret in hierarchical manner hence more secrecy is maintained in the shares. Shares generated out of this scheme are expansion less.

The Proposed authentication system is the replacement for password based authentication. In traditional password based authentication mechanism, user has to remember the password and purely influenced by dictionary attack. The authenticated person can only able to got that message. Here, signature is unique pattern presented by user and two way authentication is taking place the user authenticate to the system and system authenticate to user.

1. Cryptographic Key Assumption

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. These techniques, e.g., RSA provide a secure solution but are not practical for secure EHR storage due to the requirement for an expensive public-key infrastructure (PKI) to be maintained for distributing and managing public keys and digital certificates for all healthcare providers.

2. Attribute Key Assumption

Group key distribution schemes has recently received a lot of attention from the researchers, as a method enabling large and dynamic groups of users to establish group keys over unreliable network for secure multicast communication Group Manager transmits some broadcast message, in order to provide a common key to each member of the group.

Every user, belonging to the group, computes the group key using the message and some private information. The main property of the scheme is that, if some broadcast message gets lost, then users are still capable of recovering the group key for that session by using the message they received at the beginning of a previous session and the message they will receive at the beginning of a subsequent one, without requesting additional transmission from the Group Manager. This approach decreases the workload on the Group Manager and reduces network traffic as well as the risk of user exposure through traffic analysis.

3. Key Distribution

Common group key is frequently updated to ensure secure multicast communication. It is valid only throughout one session. Group membership can change between consecutive sessions. It can vary over time, depending on security policy, group membership changes and nodes behavior. Session key changes have to be performed, with some predefined minimum frequency to protect the system from cryptanalysis attacks.

4. Key Issuing Secured Access

The data-storing center is involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The secret key is generated through the secure the data storing center the proposed scheme is to encrypt, and decrypt algorithm definitions.

5. Security Analysis

Security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption, in our system. The fraud can be repudiated only if the client can provide a different representation he knows of from the trusted authority.

VII. CONCLUSION

In this proposed modules the signature of a person is taken as input which is encrypted using hierarchical visual cryptography. By using HVC the input signature will be divided into four shares. From that any three are taken to generate key share. Another fragmentation should handover to the authenticated server. The authenticated server should maintain the generated key and fourth fragmentation. If the receiver identifies the fourth fragmentation and decrypt they got message by using HVC. It is insecure process because anybody can hack the decrypted message easily .For the secured process the authenticated server generate a password while transferring a message. The authenticated person can only able to got that message. The authenticated server checks whether the person should be authorized user or not, while starting their conversation. It provides more security and challenged for the hackers.

REFERENCES

[1] P.S. Revenkar, Anisa Anjum, “Secure iris authentication using visual cryptography”, IJCSI , vol. 7 No. 3, pp. 217–221, March 2010.

[2] Pallavi V Chavan, Dr. Mohammad Atique, and Dr. Anjali R Mahajan, “An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review” ACEEE Int. J. on Network Security, Vol. 02, No. 04, Oct 2011.

[3] Chao Wen, Yi Wu, “A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme”, International Journal of Computer Science and Network Security, Vol. 8, no. 4, pp. 128-132, April 2008.

[4] P. L. Yi Chen, “Authentication mechanism for secret sharing using Boolean operation”, International Journal of Electronic Science and Technology, vol. 10, no. 3, pp. 195–198, September 2012.

[5] Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha “Image Captcha Based Authentication Using Visual Cryptography”, IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013.

[6] Amit Sahai, Brent Waters, ”Fuzzy Identity-Based Encryption”, IJCSI , vol. 7 No. 3, pp. 217–221, April 2013.

[7] John Bethencourt, Brent Waters , ” Ciphertext-policy Attribute-Based Encryption”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.2, March 2014.

[8] Mounika Reddy.M, Madhura Vani.B “A Novel Anti Phising Framework Based on Visual Cryptography”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[9] Jae hong seoy and keita emuray”Efficient Delegation of key generation and revocation functionalities in identity-based encryption”, ACEEE, January 11, 2013**.**

[10] Rafail Ostrovsky, Amit Sahai, Brent waters” Attribute-Based Encryption with hierarchical Access Structures”, ACEEE, Vol. 2, Issue 6, October 2012.

[11] Harinandan Tunga and Soumen Mukherjee” Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

[12] Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik" Design and Implementation of Hierarchical Visual Cryptography with Expansion less Shares", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[13] W.Shieh and T.chen, "Design and Implementation of a Novel Authentication Algorithm for D-H System Based On Visual Secret Sharing Scheme", ACEEE Int. J. on Network Security, Vol. 02, No. 04, Feb 2014.

[14] F.silvestri and H.Yan,"Authentication Mechanism for Secret Sharing Using threshold secret sharing", IJCSI,Vol. 8, no. 5, pp. 128-132, April 2008.

[15] R.Blanco and S.Dinng, "Identity Based Encryption with Hierarchical Access Structures ", IJNSIA , September 2014.