Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 7 (2017), pp. 2819-2824
© Research India Publications
http://www.ripublication.com

Secure and Data Hiding Mechanism Using Biometrics Based on Face and Finger Print

P. Sharmila
B.E student, Dept of CSE, School of Computing,
Sathyabama University, Jeppiaar Nagar, Chennai, Tamil Nadu, India.

K. Amritha
B.E student, Dept of CSE, School of Computing,
Sathyabama University, Jeppiaar Nagar, Chennai, Tamil Nadu, India.

A. Viji Amutha Mary
Assistant Professor, Department of CSE, School of Computing,
Sathyabama University, Jeppiaar Nagar, Chennai, Tamil Nadu, India.

Abstract

In wireless communication we are trading very sensitive and touchy data every now and then. Which requires an authentication and remote confirmation. It was the process which validates the remote clients based on uncertainty correspondence channel. This type of verification includes the accommodation of encoded data, alongside visual and sound signals (facial pictures/recordings, human voice and so forth.). The backbone of this paper is to get the consent to access through remote verification by scrambled data information stowing away inside picture or video objects of the cover picture. This paper deals with the survey to provide a vigorous confirmation component in view of semantic division, disordered encryption and information stowing away. After the verification of that clients various demands, at first user video object (VO) is consequently divided, utilizing a head-and-body identifier. Next, one of user biometric signs is scrambled by a riotous figure. Thereafter the scrambled flag is embedded to the most huge wavelet coefficients of the VO, utilizing its Qualified Significant Wavelet Trees (QSWTs). QSWTs give both imperceptibility and critical resistance against lossy transmission and pressure, conditions that are average in remote systems. At long last, the Inverse Discrete Wavelet Transform (IDWT) is connected to give the stego-object (SO).

INTRODUCTION

In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Authentication is the process to make sure that someone or something is, in fact, what it was declared to be. In this process the credentials are cross checked with the data in database of an authorized user. If the credentials matched then the individual is authorized and allowed to access the information. There are two types of authentication.

- User authentication
- Machine authentication

  General authentication between user and system other than guest account, automatically logged in accounts and kiosk computers. Generally user will enter the id and password to get in to the system. Authentication carried out with machine credentials much similar to user id's and passwords only submited by the system in questions .They can also use digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure to prove identification while exchanging information over the Internet, like a type of digital password.

AUTHENTCATING PASSWORD USING INSECURE COMMUNICATION

An authenticated method was proposed even when the intruder can access the data and tamper or eavesdrop the user's interaction towards the system. The proposed method provides a secured unidirectional encryption and it can be implemented with a micro computer.

Problem

In remote authentication the user will send a secret password to the system. So that the system can check whether the user is authorized or not. There are three ways in which intruder can tamper the password.

- By gaining access to data stored in system.
- By eavesdropping the line connecting user and system.
- By users easily guessed password.

Excluding the last problem remaining two can be managed by any password protocol. Because the system cannot differentiate the same information provided by two individuals. To avoid this we can use voice print as the password.

Solution

This problem can be eliminated by using one way function to encode the password. Mapping of F from some set of words is said to be a one way function.

- Given a word y, it is easy to compute F(y).
- Given a word x, it is not easy to compute a word y such that x=F(y).

MULTISERVER AUTHENTICATION BASED ROBUST BIOMETRIC

Cryptography widely use the concept of chaos theory. many key agreement protocols based on chaotic map was proposed to ensure the communication security in the real world. Maximum of them was based on smart card on account. Mostly single server environment uses smart card related protocols. As the single server environment has some defects, as it was quit complicated and boring for the user when he feels like using number of network services. Because in such case he need to enter various new identity and password repeatedly. Number of multi server authentication was proposed to overcome such issues. In the existing multi server authentication more attention was given towards efficiency rather than confidentiality or more focused on message integrity to ignore efficiency. This paper deals with a robust biometric based multi server password authentication key agreement schema on chaotic maps cryptography. The password schema was more efficient and has mass merits in terms of functionality and security analysis. Additionally this schema can resist from common attacks such as guessing, reply, intruders excreta. It was more practical in terms of efficiency analysis. Chaos theory was the mathematical branch which deals with high sensitive complex systems to slight modifications in condition, so that great consequecsis may be the result of small alterations.

UNDERSTANTING PASSWORD AND IT'S BENIFITS

Password may be word, string or character used for authentication or to prove the identity to system. Passwords are generated with small sets of rules. The major goal of this paper is to find the password is good or bad. A pareses of password was developed for better understanding and to block the weak password.

PROPOSED SYSTEM ARCHITECTURE

The proposed framework design is given in the figure 3.1. The stream of proposed framework is as per the following: Arnolds encryption make the keys that trigger the entire encryption to expand security, and the encoded biometric flag is covered up in a VO, which can dependably be distinguished in current applications that include video chatting. We propose a biometric flag is scrambled by a disorganized figure. A while later the scrambled flag is embedded to the most huge wavelet coefficients of the VO, utilizing its Qualified Significant Wavelet Trees (QSWTs). We discover the Qswt estimation for to locate the high vitality band to discover the sub-band to conceal the information of scrambled signs QSWTs give both intangibility and critical resistance against lossy transmission and pressure, conditions that are regular in remote systems. At long last, the Inverse Discrete Wavelet Transform (IDWT) is connected to give the stego-question (SO). After concentrate biometric from stegno-protest verify human face and biometric with information base.

The proposed framework comprises of three principle operations: (i) Chaotic Encryption (ii) QSWT Estimation and Hiding and (iii) Extraction Process.

CONCLUSION

We have proposed an effective remote frameworks verification plot that gives the accompanying attributes: the plan gives shared confirmation amongst client and remote server, the plan keeps the situation of many signed in clients with the same login character, the plan gives an adaptable secret key change choice, where clients can change their passwords at whatever time with no help of remote server, the remote server does not require to keep up any verifier/watchword table to approve the login ask for and the plan withstands the replay, pantomime, stolen verifier, speculating, and refusal of-administration assaults. In future, the creators will attempt to keep away from the safe divert in the enrollment stage so that the proposed development would be absolutely open channel based remote frameworks confirmation, and this is an intriguing and testing expansion of the proposed work.

REFERENCES

[1] L. Lamport., "Password authentication with in secure communication". Communications of ACM, vol. 24, no. 11, 1981, pp. 770-772.

[2] IEEE P1363.2 Draft D12., Standard specifications for password-based public key cryptographic techniques. IEEE P1363 working group, 2003.

[3] X. Li, J. Ma, W. Wang, Y. Xiong and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Mathematical and Computer Modelling, vol. 58, no.1-2, 2013 pp. 85-95.

[4] M. C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", Experts Systems with Applications, vol. 41, no. 4, 2014, pp. 1411-1418.

[5] L. H. Li, I. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks", IEEE Transactions on Neural Networks, vol. 12, no. 6, 2001,pp. 1498–1504.

[6] J.K. Lee, S.R. Ryu and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards", Electronics Letters, vol. 38, no. 12, 2002, pp. 554–555.

[7] C.H. Lin and Y.Y. Lai, "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, vol. 27, no. 1, 2004, pp. 19–23.

[8] C.C. Chang and I.C. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards", ACM SIGOPS Operating Systems Review, vol. 38, no. 4, 2004, pp. 91–96.

[9] C.T Li and M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 33, no. 1, 2010, pp. 1–5.

[10] X. Li, J.W. Niu, J. Ma, W.D. Wang and C.L. Liu, (2011), "Cryptanalysis and improvement of a biometricsbased remote user authentication scheme using smart cards", Journal of Network and Computer Applications, vol. 34, no. 1, 2010, pp. 73-79.

[11] D. Mishra, A.K. Das and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards", Expert Systems with Applications, vol. 41, no. 18, 2014, pp. 8129-8143.

[12] N. M. Haller. A one-time password system. RFC 1704, 1994.

[13] A. Shimizu. A dynamic password authentication method by one-way function. IEICE Transactions on Information and Systems, Vol. J73-D-I, No. 7, 1990, pp.630-636

[14] Samuel, S.J.,Koundinya, R.V.P.,Sashidhar, K, “Service oriented secured privacy enhancement for health care applications”, International Journal of Applied Engineering Research, Volume 10, Number 3 , 2015, pp. 6207-6216.

[15] M. Sandirigama, A. Shimizu and M.T. Noda. Simple and secure password authentication protocol. IEICE Transactions on Communications, Vol. E83-B, No. 6, 2000, pp.1363-1365.