MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

GMAIL VERIFICATION SYSTEM USING ENCRYPTION PATTERN SECURITY

Kokare Snehal, Shinde Rutuja, Zadkar Pratibha, Mr.Mhanawar N.B

Computer Department, JSPM's BSP, Wagholi,Pune

Abstract: Pattern classification systems are commonly used in adversarial applications, like biometric authentication, network intrusion detection, and spam filtering, in which data can be purposely manipulated by humans to undermine their operation. As this adversarial scenario is not taken into account by classical design methods, pattern classification systems may exhibit vulnerabilities, whose exploitation may severely affect their performance, and consequently limit their practical utility. Extending pattern classification theory and design methods to adversarial settings is thus a novel and very relevant research direction, which has not yet been pursued in a systematic way. Current Gmail authentication systems do not provide enough monitoring and management for the client. In order to enhance the security and credibility, this paper we are going to propose the concept of authentication trustworthiness, gives novel description on authentication models together with its implementation details. The results of simulations demonstrate that this combination of technology and management design can satisfy the credibility and security requirement of internet banking business.

Keywords*: Encryption, security, authentication*

1. INTRODUCTION

As the carrier of the huge fund flow, internet using is very easy to be intruded illegally and viciously attacked. Presently, the internet systems are exposed to a few information security risks: clients' ID authentication, and how to ensure the confidentiality and integrity of the financial data. Considering that there are a lot of security problems in the system, the paper only focuses the security authentication model.

Plaintext message security using biometric features has been a topic of research interest by numerous research groups and researchers around the world, and many ideas and techniques have been proposed to solve this problem. However, these ideas were not as a unified solution, which can satisfy all users or can be used for general application. Well known examples of attacks against pattern ,classifiers are: submitting a fake biometric trait to a biometric authentication system(spoofing attack); modifying network packets belonging to intrusive traffic to evade intrusion detection systems (IDSs); manipulating the content of spam mails to get them past spam filters (e.g., by misspelling common spam words to avoid their detection). Adversarial scenarios can also occur in intelligent data analysis and information retrieval; e.g., a malicious webmaster may manipulate search engine rankings to artificially promote website.

2. RELATED WORK

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. “In this section, we briefly review the related work on Gmail verification system and their different techniques.

3. EXISTING APPROACH

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the algorithm for verification systems. The existing system the i.e. Gmail accounts provide security but not up till the mark. In Gmail we have username and password with which we can get access to our account. This account provide access to all who have the password and unable to hide the private data from user.

4. PROPOSED APPROACH

We are going to build the system in which enhance security will be provided to the user. The application like Gmail which will have more security by providing more security credentials within the user account.

Advantages of proposed system:

- For better Enhancement in the Application
- Authentication
- Trustworthiness

5. PROPOSED SYSTEM DIAGRAM

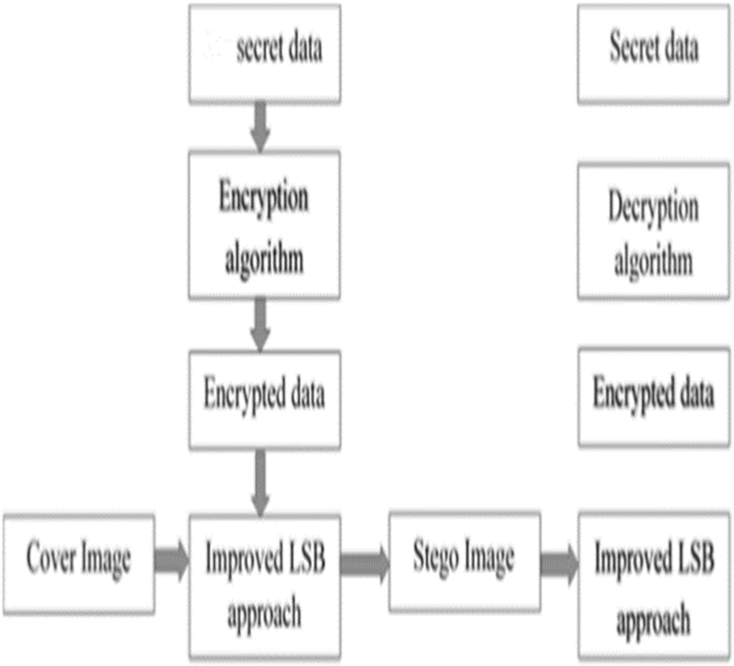

Fig 1. System Architecture

In the proposed system we have used encryption technique to verification of the user identity continuous throughout the session. To achieve we have combine different techniques such as login id and password, user image encryption which will get send to the valid mail id during the session. The system also check if screen or system stay identical for long time then again user get verify once. The main purpose of the system is to verify the user and provide security.

6. CONCLUSION

In this paper we studied system which provides various existing methods used for continuous authentication using username & password, one time password verification, figure print biometrics, random questions. Initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this system attempts to provide a comprehensive survey of research on the underlying building image encryption to build authentication. Authentication verification with image encryption improves security and usability of user session.

REFERENCES :

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[2] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 1999.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems.

[4] (SCS '08), pp. 1-6, Nov. 2008. [4] Bio ID "Biometric Authentication as a Service (BaaS)," Bio ID Press Release, https://www.bioid.com, Mar. 2011.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr.2007.