Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2337-2342
© Research India Publications
http://www.ripublication.com

A Fusion Based Authentication Technique

[1]Deepti Chilbule
Mtech, Scholar,
BIS, Bhopal,
India.

[3] Dr. Shailendra Singh
Professor & Head, Department of
Computer Engineering and Application,
N.I.T.T.T.R., Bhopal, India.

[2] Prof. Damodar Tiwari
Assistant Professor,Department of
Computer Science & Engg., BIST,
Bhopal, India.

[4]Dr. Sanjeev Sharma
Professor, SOIT, RGPV,
Bhopal, India.

I. INTRODUCTION

The Internet connectivity has converted the whole world into a global village and at the same time created many security problems. For any organization, it is essential to protect its internal resources from security threats from all over the world. Security has three important goals - confidentiality, integrity and availability. Confidentiality refers to providing access to only authorized users, integrity refers to preventing from unauthorized changes and availability refers to providing access to authorized users at any time. Confidentiality can be provided by authentication and encryption. Authentication is the first level of security for resources to prevent intruders and to provide access only to the legitimate users. It is difficult to compromise a system that has preventive measures. Intrusion is any activity that compromises the security of a system. The main aim of the intruder is to access the system resources pretending like a legitimate user either by guessing the passwords or by stealing the passwords. User authentication is the process of verifying the claimed identity of the user. By allowing only legitimate users, system access can be denied to the unauthorized users. There are three basic techniques for authentication – Knowledge based authentication, Token based authentication and Biometric based authentication. For authentication, Knowledge based authentication technique uses something the user knows (e.g. passwords), Token based authentication technique uses something the user has (e.g. smart card) and Biometric based authentication technique uses unique, measurable

characteristic of an individual (e.g. Iris, finger print). Among the three techniques, knowledge based technique is widely used for authentication because it is well known to all domains of users and easy to implement. Token based and Biometric based authentications are more secure than knowledge based authentication but, those techniques have their own limitations. Biometric authentication is not yet adopted for all applications because of the expenditure involved for maintaining the special devices required for that. In the case of Token based authentication, token should always be carried for accessing the service and there is a possibility of losing the token or the token being stolen by some body. To avoid the usage of stolen tokens, an extended token based authentication uses PIN (Personal Identification Number) in addition to tokens for authentication. In general, the three techniques can be used for different types of applications based on the security requirements. In the present situation, every user has to maintain number of user accounts either for office work or for personal work. Biometrics or Tokens can be used for applications with high security requirements and knowledge based authentication can be used for other applications. The traditional method used for knowledge based authentication is textual passwords. Passwords are widely used to authenticate users of operating systems, database systems, networks, mobile devices and application software such as email and e-commerce.

II. LITERATURE REVIEW

In [11] author proposed a multimodal biometric authentication which lies in cognitive biometrics. They use biological signals representative of the mental and emotional states to authenticate the users.

Multi-modal biometrics to allow the personal device to identify its owner and also human-like security models to facilitate dependable decision-making by the device has been proposed in [10].

In [9] an adaptive, non-obtrusive solution to secure the authentication process of cellular phone has been proposed where cellular phone learns various intrinsic attributes of the owner. Gait and location signatures of the owner are used as the metrics for the authentication.

In [4] This authentication technique is a fusion of four different authentication schemes that uses user's biometric modality, user behavior, and user physiological characteristics.The authentication process in this approach is silent and less intrusive most of the time, i.e., the authentication process runs continuously in the background until a higher level of security is needed.

Hierarchy of authentication is used to make system easy for verification. Password with facial expressions is created by extracting emotions from the expression.

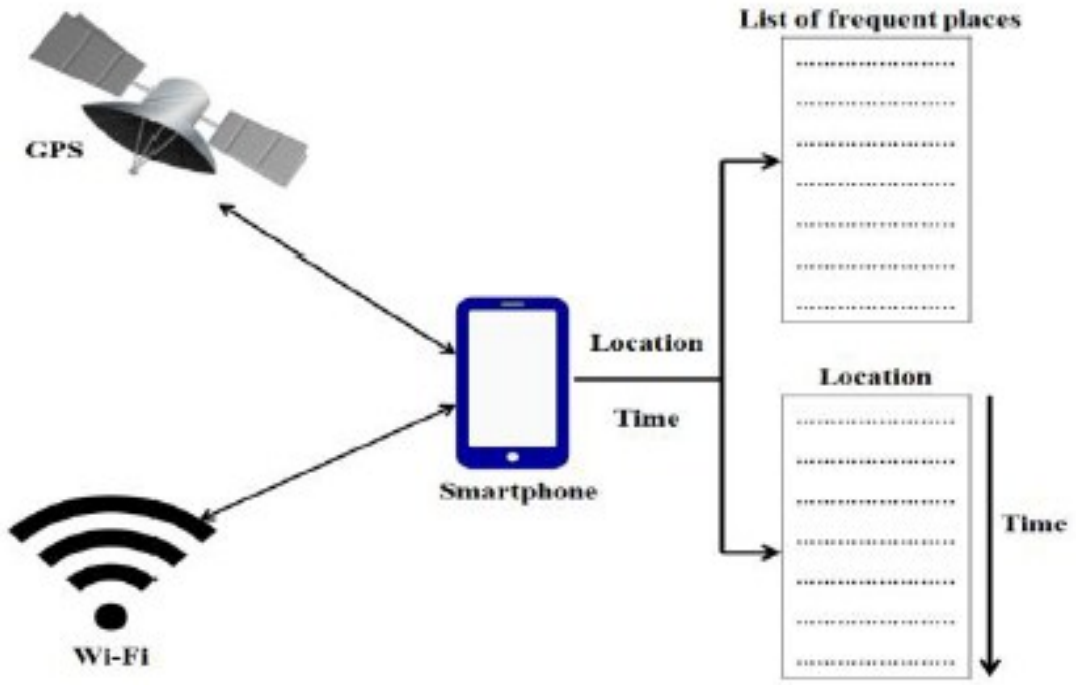
III. PROPOSED APPROACH

A hybrid scheme of authentication can be used for mobile authentication using :

- **GPS:** which will track the common locations where user moves. And will generate more levels of security when unknown location is tracked.
- **Finger Print Recognition:** Finger prints are unique for human beings. These days mobile phones comes with finger print recognition systems.
- **Smile:** Instead of extracting emotions from face, smile based authentication from facial expressions can be used with more accuracy.

PHASE 1 – GLOBAL POSITIONING SYSTEM

This module will track the location traces of user with time, which is shown in figure. The location data will be collected using GPS and Wi-Fi. Various location based services (LBS) has been developed using global positioning system (GPS) for outdoor environment and it has a higher rate of accuracy.

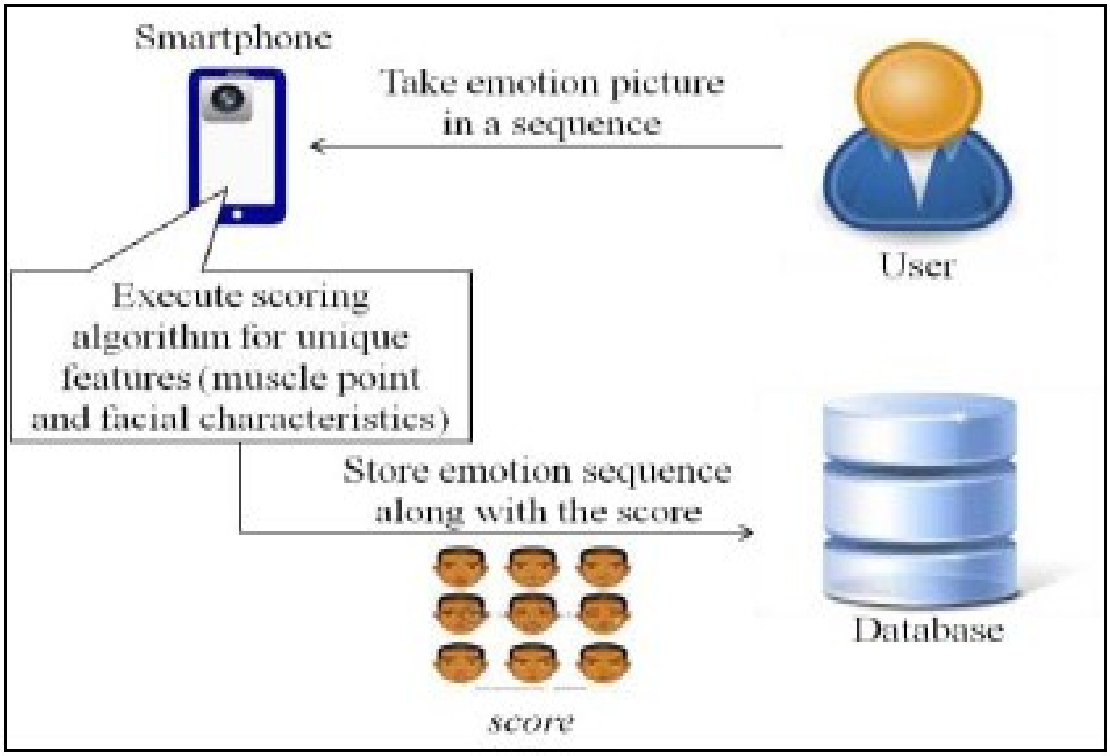


PHASE 2 – SMILE RECOGNITION

This module is responsible for authenticating a user when the silent authentication

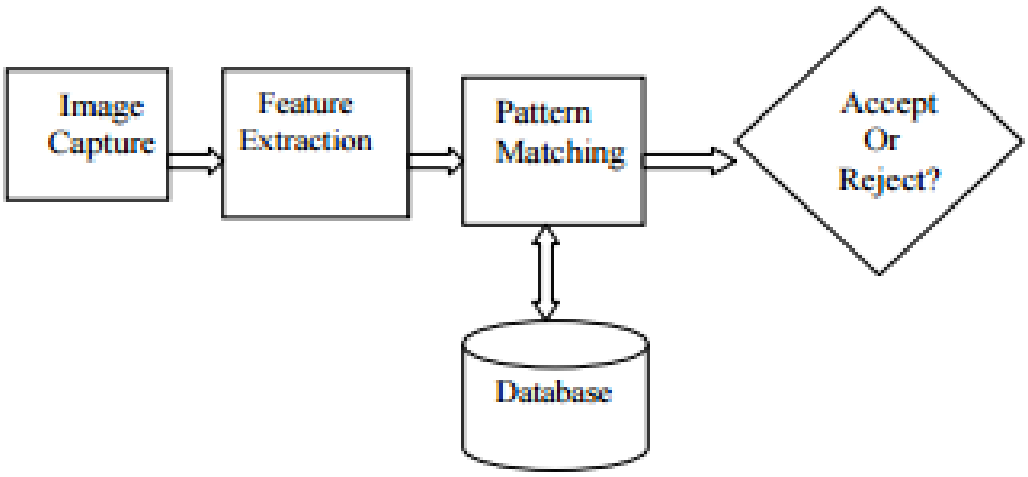
step fails. In this module, we present a novel and unique technique of user authentication based on facial expression based emotion. This authentication scheme is based on computing a "path" of known facial expression based on some unique feature related to each emotion of user.

This facial expression will be used to analyze corresponding emotion of user. The emotion sequence corresponding to user's choice facial expression will be stored in a database as their future password. In the authentication stage, the user will be asked to take pictures of his/her emotion in the exact same sequence as the emotion sequence password using the device camera. The user is authenticated if the entered emotion sequence and emotion matches with the stored one.



PHASE 3 – FINGERPRINT RECOGNITION

FP biometric is the commonly used oldest and solely method internationally accepted as legal method to identify a person. FP is the impressions of the minute ridge (called as dermal) of the finger. FP ridges and valleys are unique and unalterable. FP biometric is used in numerous applications that include civilian and commercial applications like military, law enforcement, medicine, education, civil service, forensics, driver license registration, cellular phone access.



V. CONCLUSION

This paper presents an approach to circumvent the unique challenges present in ubiquitous environments that uses mobile devices as an interface for various services and applications. We have proposed a non-obtrusive, reliable and adaptive solution to user authentication for mobile devices. We have proposed to utilize fingerprint, face and behavioral biometrics along with environmental factors to authenticate the owner of a cellular phone.

REFERENCES

[1] Biometrics for secure mobile connections. http://www.21stcentury.co.uk /technology/biometrics-formobiles. asp.

[2] Elena Vildjiounaite, Satu-Marja M¨akel¨a, Mikko Lindholm, Vesa Kyll¨onen, and Heikki Ailisto. “Increasing security of mobile devices by decreasing user effort in verification”. In ICSNC, page 80. 2007.

[3] Alejandro Quintero, "A user pattern learning strategy for managing users' mobility in umts networks", IEEE Transactions On Mobile Computing, vol. 4, no. 6, pp. 552- 556, 2005.

[4] M. Angela Sasse, “Computer security: anatomy of a usability disaster, and a plan for recovery”, In Proceedings of CHI2003 Workshop on Human-Computer Interaction and Security Systems (2003)

[5] L. F. Cranor and S. Garfinkel, “Secure or usable?”, IEEE Privacy & Security, vol. 2, pp. 16-18, 2004.

[6] A. Adams and M.A. Sasse, "Users are not the enemy,“ Comm. ACM, vol. 42, no. 12, 1999, pp. 40–46.

[7] Hafiz, M.D.; Abdullah, A.H.; Ithnin, N.; Mammi, H.K., "Towards identifying usability and security features of graphical password in knowledge based authentication technique," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.396- 403, 13-15 May 2008.

[8] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords". In SOUPS, ACM, 2006.

[9] Mohammad Tamviruzzaman, S I Ahamed, C S Hasan, C O'brien. "epet: when cellular phone learns to recognize its owner", In SafeConfig '09: Proceedings of the 2nd ACM workshop on Assurable and usable security configuration, pages 13–18, Chicago, IL, USA, 2009. ACM.

[10] R. Greenstadt and J. Beal. "Cognitive security for personal devices", In the First ACM Workshop on AISec, 2008.

[11] Vítor J. Sá, "Gesture dynamics with skin conductivity – a multimodal approach to biometric authentication", Week of the school of Engineering, [Semana da Escola de Engenharia], October 24 - 27, 2011.

[12] M. Jakobsson, E. Shi, P. Golle, and R. Chow. "Implicit authentication for mobile devices", In HotSec'09: Proceedings of the 4th USENIX conference on Hot topics in security, pages 9–9, Berkeley, CA, USA, 2009. USENIX Association.

[13] Hu Xing; Jie Zhou; Lijun Dong; "The study of localization algorithm based on RSSI," Information Science and Technology (ICIST), 2011 International Conference on , vol., no., pp.766-769, 26-28 2011.

[14] Farzana Rahman, Md Osman Gani, Golam Mushih Tanimul Ahsan and Sheikh Iqbal Ahamed "Seeing beyond visibility: A Four Way Fusion of User Authentication for Efficient Usable Security on Mobile Devices" in 2014 Eighth International Conference on Software Security and Reliability – Companion.