**Persistent user authentication system by using RFID, Ultrasonic sensor and human behavioral characteristics**

Prashant Shinde \*, Sham Kale \*, Bhavesh Parab \*, Ravindra Prasad \*, Prof. Bhushan Chaudhari

# Department of Information Technology, Sandip Institute of Technology and Research center  
Mahiravani, Trimbak Road, Nashik-422213, Maharashtra, India

Email: [info@sitrc.org](mailto:info@sitrc.org) Website: www.sandipfoundation.org

Savitribai Phule Pune University

[www.unipune.ac.in](http://www.unipune.ac.in/)

Abstract— **A review on Persistent user authentication system using RFID, Ultrasonic sensor and behavior characteristics. Now days most of the security system uses traditional methods for the authentication for example by providing user name and password ,smart cards etc but in these techniques the user verified only one time at the initial logging, after that he can access all the resources until he logout. This will lead to session hijacking if authenticated user takes short break the hoaxer can gain the control over system. To overcome these issues we have to use system that should continuously examine the user for assuring the user authority. Current System continuously examine user using multi modal biometrics but still there are some issues such as we all know that face detection is not 100 % accurate there are some constraints with it, and all these done using image processing and it contains some flaws. Also user can’t afford such expensive system. To overcome all these issues we proposed cost effective system, which will continuously monitors user and detect whenever user leaves workstation. For that we are going to used RFID for unique identification, Ultrasonic sensor to detect presence of user in front of computer System and keystroke dynamics that will checks the behavior of user which are unique for each user so it will provide highest security as compare to exiting logging systems the new thing in our system that we going to used RFID and Ultrasonic sensor in which there is no need to do image processing, whenever user leaves workstation system will logout immediately. This**

**will provide highest security to the system and resources.**

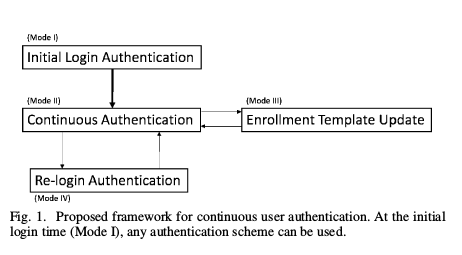
Keywords**—** RFid, Ultrasonic Sensor, Keystroke detection.

**Introduction**

Persistent user authentication system that continuously monitors user based using RFID ,Ultrasonic Sensor and keyboard dynamics. The primary objective of the Persistent authentication system is to prevent impostor or third party from gaining access to the system while user takes short break from workstation. Our system first register user with RFID tag and keystroke behavior and when user going to access system, it will check for RFID tag initially, after that Ultrasonic sensor and keyboard dynamic module gets activated. Ultrasonic sensor checks presence of user in front of computer system and keyboard dynamic module checks typing habits of the user. Any changes in typing habits are detected then systems will immediately logouts. Also whenever user leaves workstation it will be detected by ultrasonic sensor and system will logout immediately.

Conventional verification systems, such as those controlling access to a secure room or particular system, do not usually require the user to re-authenticate him for continued access to the protected resource. This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized use. In such cases, continuous verification is needed. The proposed system continuously verifies the presence of a logged-in user using ultrasonic sensor. Three modalities are currently used face, fingerprint and heartbeat but our theory can be readily extended to include more modalities like RFID for unique identification, ultrasonic sensor for continuously checking presence of user. There has been an increasing demand for on-line activities such as e-banking, e-learning and e-commerce. However, these on-line activities continue to be marred by evolving security challenges. On-line verification is now central to security discussions. The use of biometrics for individual authentication has always existed. Physiological biometrics, which is based on physical features, is a widespread practice. Behavioral biometrics, however, is based on what we do in our day-to-day activities such as walking or signing our names. Current research trends have been focusing on behavioral biometrics as this type of authentication is less intrusive. Hepatics have come a long way since the first glove or robot hand. Hepatics have played an immense role in virtual reality and real-time interactions. Although gaming, medical training and miniaturization continue to prove the enrichments created by hap tic technology, as hap-tic devices become more obtainable, this technology will not only serve to enhance the human-computer interface but also to enhance cyber security in the form of on-line biometric security. Hepatics have come a long way since the first glove or robot hand. Hepatics have played an immense role in virtual reality and real-time interactions. Although gaming, medical training and miniaturization continue to prove the enrichments created by hap-tics technology, as hepatic devices become more obtainable, this technology will not only serve to enhance the human-computer interface but also to enhance cyber security in the form of on-line biometric security. Limited research has been done on the combination of hepatics and biometrics. To date, dynamic on-line verification has been widely investigated using devices which do not provide the user with force feedback. Hap-tics technology allows the use of force feedback as an additional dimension. This key behavioral biometric measure can be extracted by the hepatics device during any course of action. This research has significant implications for all areas of on-line verification, from financial applications to gaming. Future challenges include incorporating this technology seamlessly into our day to day devices and operations. Humans used different body characteristics such as face, voice, and gait for thousands of times to recognize each other. By all these we conclude that every system mention has issues either of performance or cost in that case our system will best. Now days in most of the computer system the authentication of the user is examine only at initial login, the system and its resources are made available for the user until he/she is logged in. This could be a critical security weakness for high ­security systems because it allow hoaxer to gain a access to the system until the initial user logs out. This condition encountered when the authenticated user take short break without logging out or hoaxer forces valid user to gain an access to system. To overcome this security flaw, we need to continuously examine the user, to achieve this objective, proposed Persistent user authentication system that continuously monitors user using RFID ,Ultrasonic Sensor and keyboard dynamics. That continuously examines and authenticates the logged in user using RFID and keyboard dynamics, Presence detection using ultrasonic sensor. The project focuses on the problem of initial login or one time authentication. There are various approaches for initial login such as user name and password, smart card, IDs etc. but password is difficult to remember and smart card can be shared, stolen or lost. To circumvent these problems, a number of login authentication methods, like textual type and graphical passwords, public key infrastructure (PKI), and biometric authentication, have been utilized. All of the above login methods create common problem that namely authenticate a user only at the initial login session and do not re authenticate a user until the user logs out or there is a substantial time interval between user’s activities on the workstation. This could pose a critical security weakness not only for high security system, but also for personal computers in a general office environment. To overcome these flaws, we need a system that continuously monitor or examine user for authentication. The idea is to design a Persistent user authentication system that continuously monitors user based using RFID, Ultrasonic Sensor and keyboard dynamics. In this we examine user using RFID, keystroke while typing and checks presence of user using Ultrasonic sensor in front of computer system, whenever user leaves workstation system will logout automatically.

Our method automatically registers the user every time the user logs in. We also used continuous authentication method by addressing the issues in the concerning re login authentication which checks short absence of the particular user.



In future there is scope to add module of digital signature. Considering our current idea will provide highest security in cost effective way as compare to existing initial login and continuous multi-model biometric systems.

**II. LITERATURE SURVEY**

This survey aims at providing multimedia researchers with a state-of-the-art overview of fusion strategies, which are used for combining multiple modalities in order to accomplish various multimedia analysis tasks. The existing literature on multi-modal fusion research is presented through several classifications based on the fusion methodology and the level of fusion (feature, decision, and hybrid).Numerous studies have been done on dynamic signature verification – Plamondon (Plamondon & Srihari, 2000) and Jain (Jain et al., 2002) are just two of the popular names associated with these studies. Some of the work done on DSV follows. In a study by Lee et al. (1996) individual feature sets as well as individual thresholds were used. The authors suggested that if time is an issue then a common feature set should be used. These features were captured using a graphics tablet (or digitizing tablet, graphics pad, drawing tablet). Normalization was done using factors such as total writing time (time- normalized features), total horizontal displacement, and total vertical displacement. Majority classifiers (implementing the majority decision rule) were used in the classification stage .The single biometric system is most widely used in various applications. On account of the limitations raised by the single biometric system many users resorted to multimodal biometric system in order to provide maximum level of accurate authentication. Effective utilization of the advantages of multiple biometric traits is applied to enhance the performance in many aspects including accuracy, noise resistance, and universality, spoof attacks, and reduce performance degradation in huge database applications. Nowadays, new algorithms and applications of multi-modal biometrics are emerging tremendously. The most commonly used biometrics is face, that is, either as a single trait or combined with other trait as multi modal biometrics. Face combined with other biometrics at different level of fusion. From the literature survey it is inferred that the different fusion levels and combinations of different biometric modalities are being used by different researchers are for accurate personal identification. Also the performance metrics used for quality -based multi - modal biometric system, fusion approaches must be carefully selected as the precision in personal identification or verification rate may be affected. All performance metrics are not made applicable for all the four fusion levels. There is a scope for better evaluation framework for biometric quality assessment metrics by correlating with the available fusion schemes. Also computational cost in the development of quality assessment approach shall be reduced. Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users. For decades, many highly secure environments have used biometric technology for entry access. Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings).Biometric system which relies on the

Evidence of multiple sources of information for establishing identity is called Multi-modal biometric system. This paper presents an overview of multi-modal biometrics, challenges faced by multi-modal biometric system. It also discusses their applications to develop the security system for high security areas. We also discuss the application of biometric systems and their advantage over single biometric system. Biometrics permits unmanned access control. Biometric devices, typically hand geometry readers, are in office buildings, hospitals, useful for high-volume access control. A lot of research work is still need in this area. In near future combination of more than two biometrics can apply to enhance the security of our system.

**III.PROBLEMS AND CONSTRUCTION WORK**

*3.1 Problems*

1. Initial logging systems checks authentication at the start of the session and after that re-authentication is not done using RFID.
2. It is not possible to provide prompting message box after specific time interval for authentication because users get distracted from their work.
3. For on-line transaction this initial authentication system can leads to session hijacking, because after initial checking re-authentication is not done.
4. If user after initial authentication takes a short break from work station then during that time the hoaxer can obtain the access to the system.
5. Using only textual authentication the user can not uniquely identifies, because the passwords and smart cards can be shared and stole.

*3.2 The main research content*

The plan for work has begun with studying about all existing login system and their flaws. Study and examine the research work done in the field of security using the biometric. The Field study and Background work related to Ethics and Law needs to be studied and the later part consists of hardware constraints and software challenges will be in consideration. Then we are going to design the algorithm for integrating the physiological characteristics.

*3.3 Proposed working*

The proposed system calculates score when user login at first time and then those readings are store into database at the back end. The score generated by different algorithms in different module with the distinct hardware, are integrated by integrator and

Then analysis of those scores are perform based on the designed algorithm after this analysis the scores

Are match with the database at the back-end and then controller takes the decision that the particular user is authenticated or not.

 **Algorithms**

Authentication is done under following algorithms

1. Initial login using RFID

2. Ultrasonic Sensor checks for Presence of user

3. Keystroke monitoring

The above algorithms observe the human behavior and generate a score after initial login. Initial login will be done with RFID, ultrasonic checks for presence of user in front of system, Typing scores are calculated using keyboard dynamics in this way the scores are generated.

B. Working

The proposed system calculates score when user login at first time and then those readings are store into database at the back end. The score generated by different algorithms in different module with the distinct hardware, are integrated by integrator and

Then analysis of those scores are perform based on the designed algorithm after this analysis the scores

Are match with the database at the back-end and then controller takes the decision that the particular user is authenticated or not.

C. Expected Outcomes:

1) The existing system suffers from the problem of session hijacking that should resolve using continuous authentication.

2) The proposed system should provide high-security for the on-line user as well as to the personal computers.

3) The system should provide high security to the system using RFID.

4) Project should calculate the keystroke score of the user on the initial logged-in and also calculate the fingerprint score of the user and then these scores should integrate by integrator.

5) User profile of the user will form and when particular user try to access system next time the system will check for the continuous authentication of the user.

6) When user try to access again then the pattern matching will performs between the new pattern and the old that are stored into system's database

7) Project should provide the high-security to the using continuous authentication by integrating the physiological characteristics of the user.

D. Feasibility Study:

The proposed project is planned on the foundation of the open source hardware and applications. The means of Open source adaption proves flexibility of system for working. The cost factor, when kept in consideration, the proposed method will accomplish in 30,000/- but may reduce or increase as and when challenges cannot be predicted. The idea provides highest level of security to system and overcomes the flaws of traditional initial logging system.

1. **Conclusion**

The chapter shows that the potential for greater accuracy for on-line verification as well as stand-alone systems exists with the use of human physiological characteristics by extracting data which is available from the digital tables in use as well as force data. Though experimental data using hepatics devices are limited, the experiments covered showed that verification accuracy is at very high level but still there are some flaws in the system and also there not cost effective, our idea will provide highest security to system in lowest cost with RFID for initial login ,Keyboard dynamics and ultrasonic sensor for detecting presence of user in front of system ,this will be best and cost effective solution to overcome flaws of the existing system.

**V. REFERENCES**

[1] R. Bolle A. Jain and S. Pankanti. Biometrics: Personal identification in a network society.MA: Kluwer Academic Publisher, Norwell, 1999.

[2] J. Liu, FR Yu, C.H. Lung, and H. Tang. A Framework of Combining Intru-sion Detection andContinuous Authentication in Mobile Ad Hoc Networks. In IEEE International Conference onCommunications, 2008. ICC’08, pages1515–1519, 2008.

[3]A. Peacock, X. Ke, and M. Wilkerson. Typing patterns: A key to user identification.IEEE Security and Privacy, pages 40–47, 2004.

[4] Anil K.Jain Computer Science and Engineering Department, Michigan Statte University, East Lansing, MI.

[5] Anil K.Jain, Soft Biometric Traits for continuous user Authentication, In IEEE Transactions on information forensics and security,1556-6013, 2010 IEEE.

[6] Arun Ross and Salil Prabhakar,An Introduction to Biometric Recolonization, In IEEE Transactions on cicuits and system for video technology,1051-8215,2004

[7]Khalil Challita ,Hikmat farhat, Biometric authentication for Intrusion Detection system,In IEEE first international Conference on Integrated Intelligent Computing, 978-0-7695-4152- 5,2010.

[8]M. Pusara and C.E. Brodley. User re-authentication via mouse movements. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 1–8.ACM New York, NY, USA, 2004.

[9]K. Revett, F. Gorunescu, M. Gorunescu, M. Ene, S. Magalhaes, and H. San-tos. A machine learning approach to keystroke dynamics based user authentication. International Journal of Electronic Security and Digital Forensics,1(1):55–70, 2007.

[10] A. Ross and A. Jain. Biometric sensor interoperability: A case study in fingerprints. Lecture notes in computer science, pages 134–145, 2004.

**Web references**

[1]http://www.researchgate.net/publication/224174218\_Soft\_Biometric\_Traits\_for\_Continuous\_User\_Authentication.

[2]http://dl.acm.org/inst\_page.cfm?id=60031707&CFID=695924067&CFTOKEN=56426513

[3]<http://www.realtimebiometrics.com/solutions.html>

[4] http://www.realtimebiometrics.com/news.html