Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on User Identity Verification for Secure Login Session

[1]Swati Borude, [2]Pratiksha Chokhar, [3]Neha Bhosale, [4]Ashwini Palve, [5]Prof. M. N. Kale
[1, 2, 3, 4]IT Dept, DVVPCOE, Ahmednagar, Maharashtra, India
[5]Asst.Prof.IT Dept, DVVPCOE, Ahmednagar, Maharashtra, India

Abstract— In web applications, user authentication is normally based on username and password, come forth biometric solutions allow biometric data during session establishment. But in Unimodel biometric approaches only use a single verification is considered and the identity of the user is permanent during the entire session. A secure protocol is defined for constant authentication through continuous user verification. Biometric techniques suggest solution for secure, trusted and protected authentication. In between the logging session time, the one-time-password (OTP) is send on users registered email id and also randomly one questions will be asked to the user between the 5-10 mints. The user's identity has been verified, the system resources are available for fixed period of time and identity of the user is constant during entire session. The proposed system detects misuses of computer resources and prevents malicious activities based on multi-modal biometric continuous authentication. Biometric and user information's are stored in smart phones and web services.

Keywords— Authentication, Security, Mobile environments, web servers

I. INTRODUCTION

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits, Gmail OTP verification and users personal information. Biometrics is the science and technology of determining identity based on physiological and behavioural traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors[1][2].

In fact, similarly to traditional authentication processes which rely on username and password with OTP verification, biometric user authentication is typically formulated as a single shot, providing user verification periodically during login time when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach is also susceptible for attack because the identity of the user is constant during the whole session[2][3]. Suppose, here we consider this simple scenario: a user has already logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution. So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric continuous authentication and personal question verification are proposed, that means turning user verification into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one[2][3][4].

II. LITERATURE SURVEY

Andrea Ceccarelli, Leonardo Montecchi "Continuous and Transparent User Identity Verification for Secure Internet Services" IEEE TRANSACTIONS MAY/JUNE 2015. In web applications, user authentication is normally based on username and password, come forth biometric solutions allow biometric data during session establishment. but in Unimodal biometric approaches only use a single verification is considered and the identity of the user is permanent during the entire session. A secure protocol is defined for constant authentication through continuous user verification. Biometric techniques suggest solution for secure, trusted and protected authentication. In between the logging session time, the one time password (OTP) is send on users registered email id and also randomly one questions will be asked to the user between the 5-10 mints. The user's identity has been verified, the system resources are available for fixed period of time and identity of the user is constant during entire session. This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through

continuous user verification. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The functional behaviour of the protocol is illustrated through Matlab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers[4][5].

Elizabeth LeMay, Willard Unkenholz, "Adversary-Driven State-Based System Security Evaluation" MetriSec2010 September 15, 2010, Bolzano-Bozen, Italy. This paper describes the system and adversary characterization data that are collected as input for the executable model. This paper also describes the simulation algorithms for adversary attack behaviour and the computation for the probability that an attack attempt is successful. A simple case study illustrates how to analyze system security using the ADVISE method. A tool is currently under development to facilitate automatic model generation and simulation. The ADVISE method aggregates security-relevant information about a system and its adversaries to produce a quantitative security analysis useful for holistic system security decisions. The system doesn't apply the ADVISE method to evaluate the security of a whole company's system architecture. A security analysis tool using the ADVICE method is currently under development[5][6].

S.kumar, T.sim "Using Continuous Biometric Verification to Protect Interactive Login Sessions", 2012. This paper we describe the theory, architecture, implementation, and performance of a multi-modal passive biometric verification system that continually verifies the presence/participation of a logged-in user. We assume that the user logged in using strong authentication prior to the starting of the continuous verification process. While the implementation described in the paper combines a digital camera-based face verification with a mouse-based fingerprint reader, the architecture is generic enough to accommodate additional biometric devices with different accuracy of classifying a given user from an imposter. The main thrust of our work is to build a multi-modal biometric feedback mechanism into the operating system so that verification failure can automatically lock up the computer within some estimate of the time it takes to subvert the computer. This must be done with low false positives in order to realize a usable system. This system For all biometrics there is a trade-of between computation and the Verifier's Power. It requires more computation for a single assessment output And for continuous verification it can add a factor to the computational load[6][7].

D.M.Nicol,W.H.Sanders, "Model-Based Evaluation: From Dependability to Security", IEEE TRANSACTIONS 2004. In this work, we survey existing model-based techniques for evaluating system dependability, and summarize How they are now being extended to evaluate system security. We find that many techniques from dependability evaluation can be applied in the security domain, but that significant challenges remain, largely due to fundamental differences between the accidental nature of the faults commonly assumed in depend ability evaluation, and the intentional, human nature of cyber-attacks. This system identifying modelling attacker behavior determining the appropriate level of detail/abstraction in an attacker model is very important. But it is difficult to determine[8].

T. Sim, S. Zhang, R. Janakiraman , and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Apr. 2007. In this paper we describe a system that continually verifies the presence/participation of a logged-in user. This is done by integrating multimodal passive biometrics in a Bayesian framework that combines both temporal and modality information holistically, rather than sequentially. This allows our system to output the probability that the user is still present even when there is no observation. Our implementation of the continuous verification system is distributed and extensible, so it is easy to plug in additional asynchronous modalities, even when they are remotely generated. Based on real data resulting from our implementation, we find the results to be promising. This system is continuously verification of bio-metric may get tedious to user[9][10].

III. PROPOSED SYSTEM

In the proposed system we have used CACHMA system to verification of the user identity continuous throughout the session. To achieve we have combine different techniques such as login id and password, user biometrics and also OTP 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 CACHMA is to verify the user and send the certificate to the web services[11][12].

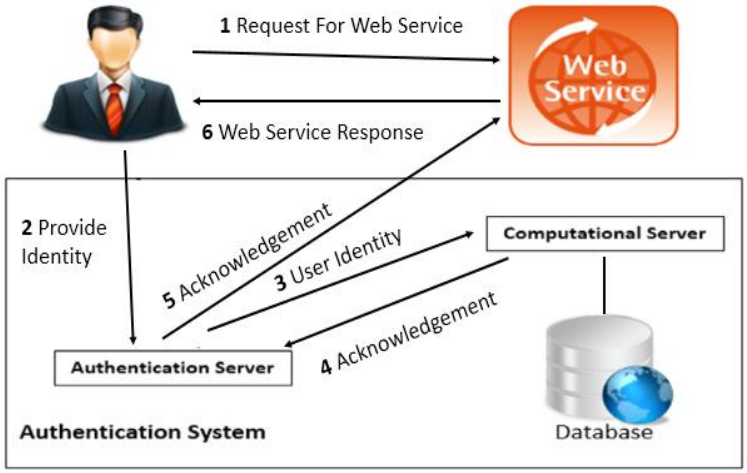

Fig 1: System Architecture

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits, Gmail OTP verification and users personal information. Biometrics is the science and technology of determining identity based on physiological and behavioral traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics[12]. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors. In fact, similarly to traditional authentication processes which rely on username and password with OTP verification, biometric user authentication is typically formulated as a single shot, providing user verification periodically during login time when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider this simple scenario: a user has al-ready logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily[10][11][12]. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution. So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric continuous authentication and personal question verification are proposed, that means turning user verification into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one[13][14].

IV. CASHMA SYSTEM

Context-Aware Security by Hierarchical Multilevel Architectures This system used for secure biometric authentication on the internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services. Depending on the preferences and requirements of the owner of the web service the CASHMA authentication service replace the traditional authentication service[14].

Algorithm for Bio- Metric verification

```
for x = 0 to image. size:
  for y = 0 to image. Size:
     diff += abs (image1.get(x, y).red - image2.get(x, y).red)
     diff += abs (image1.get(x, y).blue - image2.get(x, y).blue)
     diff += abs (image1.get(x, y).green - image2.get(x, y).green)
   end
 end
return ((float)(diff)) / ( x * y * 3)
```

Computation of trust in subsystem - The algorithm starts computing the trust in the subsystems. Intuitively, the subsystem trust level could be simply set to the static value mðSk; tÞ ¼ 1 _ FMRðSkÞ for each unimodal subsystem Sk and any time t (we assume that information on the subsystems used, including their FMRs, is contained in a repository accessible by the CASHMA authentication server)[12][13][14].

$M(s_k,t)=m(s_k,t_{i-1}).penalty(x,h))^{-1}$

Computation of trust in user - This leads us to model the user trust level through time using a function which is asymptotically decreasing towards zero. Among the possible models we selected the function in (1), which: i) asymptotically decreases towards zero; ii) yields trustðti_1Þ for D ti ¼ 0; and iii) can be tuned with two parameters which control the delay ðsÞ and the slope ðkÞ with which the trust level decreases over time[14][15].

$$G(t_i)=\frac{\left(-\arctan\left((\Delta t_i - s).k\right)+\frac{\pi}{2}\right).trust\,(t_i-1)}{-\arctan(-s.k)+\frac{\pi}{2}}$$

$$\Delta t_i = t_i - (t_i - 1)$$

Global trust level - The global trust level in the maintenance phase is a linear combination of the user trust level and the subsystem trust level. Given the user trust level gðtiÞ and the subsystem trust level mðSk; tiÞ, the global trust level is computed again adopting the OR-rule from [2], this time with only two input values. Result is as follows[15]:

$Trust(t_i)=1-(1-g(t_i))(1-m(s_k,t_i))$

$=g(t_i)+m(s_k,t_i)-g(t_i)m(s_k,t_i)$

$=g(t_i)+(1-g(t_i))m(s_k,t_i)$

Computation of session timeout - By solving for Ti, we finally obtain Equation (4), which allows the CASHMA service to dynamically compute the session timeout based on the current global trust level. The initial phase and the maintenance phase are computed in the same way: the length Ti of the timeout at time ti for the user u is[15]:

$$T_i = \int_0^{tan} \left(\frac{g_{min.(\arctan(-s.k)-\frac{\pi}{2})}}{trust(t_i)}+\frac{\pi}{2}\right).\frac{1}{k} + s \quad \text{if } T_i > 0$$

Otherwise $M(s_k , t) = 1 – FMR (s_k)$

Trust Levels and Timeout Computation - The algorithm to evaluate the expiration time of the session executes iteratively on the CASHMA authentication server. It computes a new timeout and consequently the expiration time each time the CASHMA authentication server receives fresh biometric data from a user. Let us assume that the initial phase occurs at time t0 when biometric data is acquired and transmitted by the CASHMA application of the user u, and that during the maintenance phase at time ti > t0 for any i ¼ m new biometric data is acquired by the CASHMA application of the user u (we assume these data are transmitted to the CASHMA authentication server and lead to successful verification[15][16]

Computation of the Session Timeout - The last step is the computation of the length Ti of the session timeout. This value represents the time required by the global trust level to decrease until the trust threshold gmin. Such value can be determined by inverting the user trust level function (1) and solving it for D ti[16].

V. RESULTS

User request to access web service. User needs web service access certificate. Web service checks for user authentication, CASHMA system generate the certificates. CASHMA system accepts user information and computes it. CASHMA system validates this user information (i.e. user id, bio-metric verification, answer of questions) from database. A certificate is sends towards the web service.

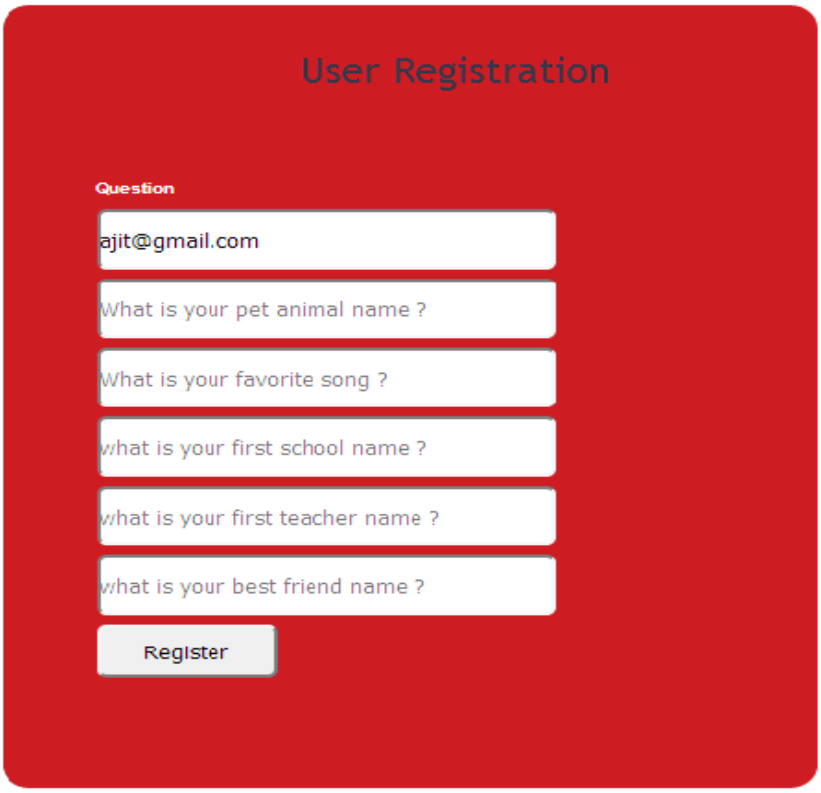

Fig 2: User Registration

Fig 3: User Login

Fig 4: Certificate Generated

Fig 5: CASHMA Certificate

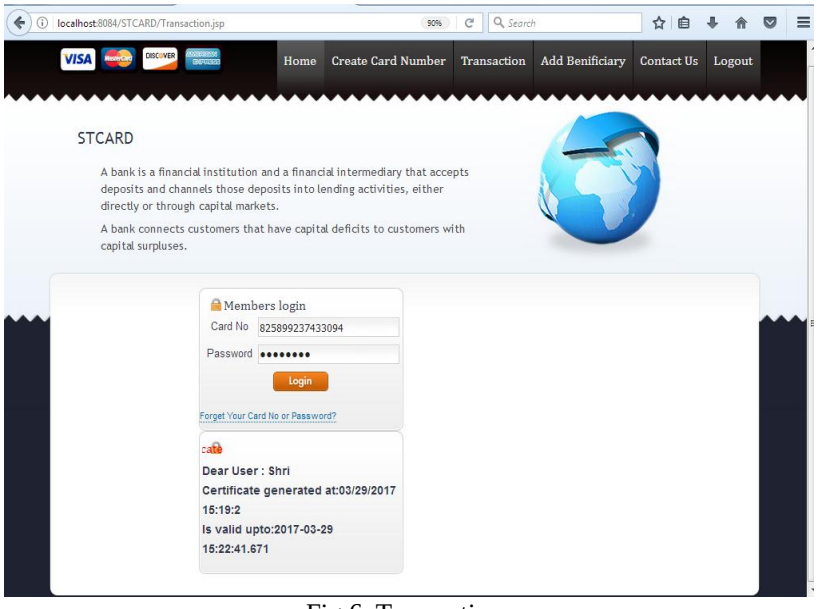

Fig 6: Transactions

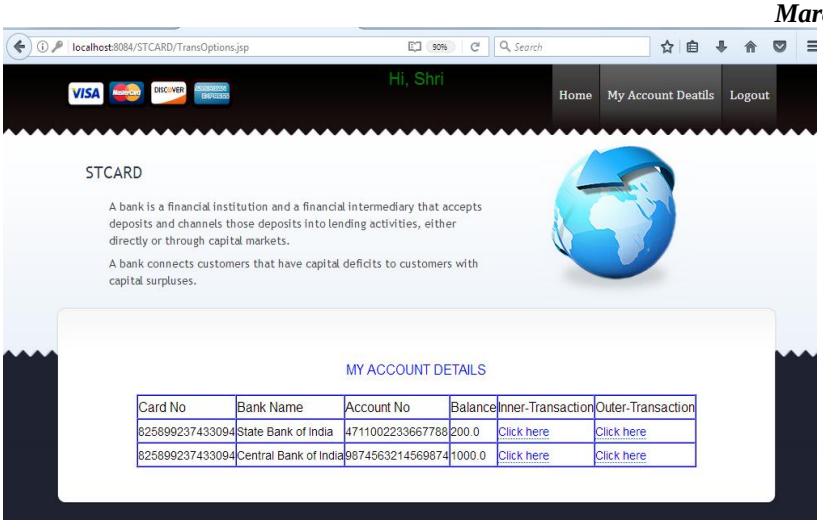

Fig 7: Account Details

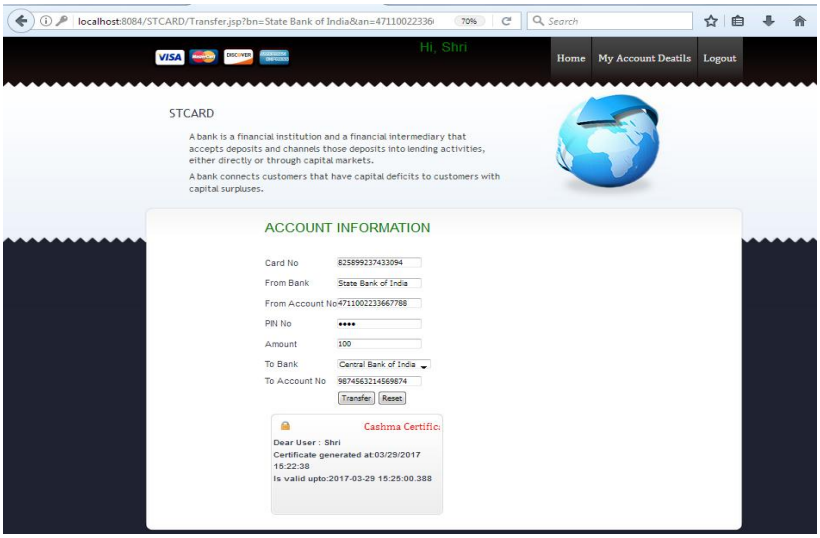

Fig 8: Inner Transactions

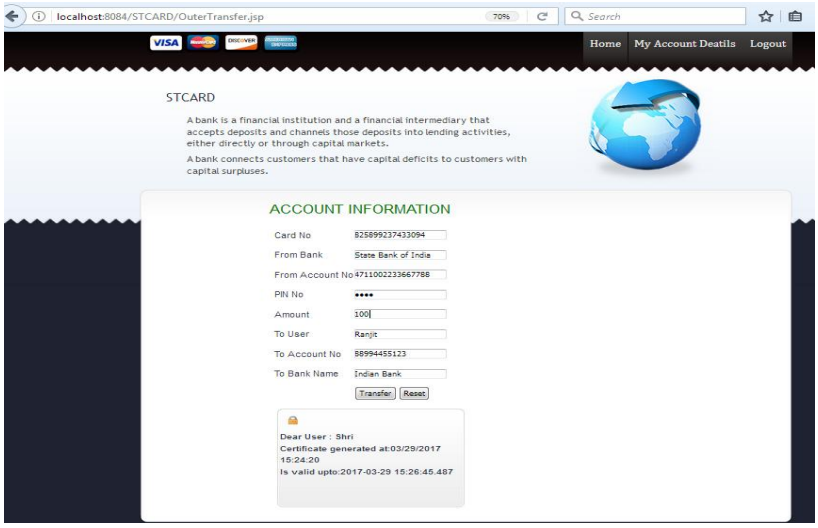

Fig 9: Outer Transactions

VI. CONCLUSIONS

In this paper we studied system which provides various existing methods used for continuous authentication using username & password, OTP verification, fingerprint 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 blocks required to build a biometric authentication continuous OTP and Random question system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

ACKNOWLEDGMENT

It is our advantage to acknowledge with deep sense of gratitude to our project guide Prof. Ms. M.N. Kale whose supervision, inspiration and valuable discussion has helped us to complete our project. Their guidance proved to be the most valuable to overcome all the complications in the fulfillment of this project on "A Survey on User Identity Verification for Secure Login Session". We are thankful to Principal Dr. Jayakumar Jayaraman or direct or indirect help in the completion of this project. Last but not least, this acknowledgement would be incomplete without rendering our sincere gratitude to all those who have helped us in the completion of this project.

REFERENCES

[1] Vidhate, Deepak A and Kulkarni, Parag "Innovative Approach Towards Cooperation Models for Multi-agent Reinforcement Learning (CMMARL)", Springer Nature series of Communications in Computer and Information Science, Vol. 628,pp. 468-478,2016

[2] Vidhate, Deepak A and Kulkarni, Parag "New Approach for Advanced Cooperative Learning Algorithms using RL Methods (ACLA)" Proceedings of the Third International Symposium on Computer Vision and the Internet, ACM, pp 12-20, 2016

[3] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[4] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

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

[6] Vidhate, Deepak A and Kulkarni, Parag "Multi-agent Cooperation Methods by Reinforcement Learning (MCMRL)", Elsevier International Conference on Advanced Material Technologies (ICAMT)-2016}No. SS-LTMLBDA-06-05,2016

[7] 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.

[8] Vidhate, Deepak A and Kulkarni, Parag "Performance enhancement of cooperative learning algorithms by improved decision making for context based application", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)IEEE Xplorer, pp 246-252, 2016

[9] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environnent," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[10] 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.

[11] Vidhate, Deepak, A; Kulkarni, Parag (2014):"Improvement In Association Rule Mining By Multilevel Relationship algorithm" in International Journal of Research in Advent Technology, 2(1), pp.366-373

[12] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

[13] Vidhate, Deepak, A; Kulkarni, Parag (2014):" A Novel Approach to Association Rule Mining using Multilevel Relationship Algorithm for Cooperative Learning" Proceedings of 4th International Conference on Advanced Computing & Communication Technologies (ACCT-2014), pp 230-236

[14] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.

[15] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

[16] Vidhate, Deepak, A; Kulkarni, Parag(2014): "Multilevel Relationship Algorithm for Association Rule Mining used for Cooperative Learning" in International Journal of Computer Applications, 86(4), pp.20-27

