Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Continuous With Visible Consumer Individuality Certification for Safe Internet Services

Jadi Vasantha
Assistant Professor,
Department of CSE,
VIF College of Engineering and Technology.

Akhil Mohd
Assistant Professor,
Department of CSE,
VIF College of Engineering and Technology.

Manjula. A
Associate Professor & HOD,
Department of CSE,
VIF College of Engineering and Technology.

ABSTRACT:

Session supervision in distributed Internet services is usually based on username and password, plain logouts and mechanisms of user session expiration using typical timeouts. Emerging biometric solution agree to substitute username and password with biometric data during session establishment, but in such an approach still a single confirmation is deemed enough, and the identity of a user is considered absolute during the whole session. Additionally, the extent of the session timeout may blow on the usability of the service and resulting client approval. This paper explore promising alternative 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 clearly acquired from the user. The useful behavior of the protocol is illustrated through Matlab simulation, while model-based quantitative analysis is carried out to assess the ability of the procedure to contrast security attacks exercised by different kinds of attacker. Finally, the current sample for PCs and Android smart phones is discussed.

EXISTING SYSTEM:

- One time the user's individuality has been verified, the scheme resources are accessible for a fixed period of time or until explicit logout from the user. This approach assume that a single verification (at the beginning of the session) is enough, and that the individuality of the user is constant during the complete session.
- In obtainable, a multi-modal biometric confirmation scheme is considered and developed to detect the physical presence of the consumer logged in a computer.
- The occupation in one more existing paper, propose a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, wherever the raw data acquired are subjective in the user verification process, based on i) type of the biometric traits and ii) time, since different sensors are able to provide raw data with different timings. Point ii) introduces the require of a sequential integration method which depends on the ease of use of past observations: based on the supposition that as occasion passes, the assurance in the acquired (aging) values decrease. The paper applies a corruption function that actions the uncertainty of the achieve computed by the verification function.

DISADVANTAGES OF EXISTING SYSTEM:

- None of obtainable approaches ropes unbroken authentication.
- Rising biometric solution allow substitute username and password with biometric data throughout session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session.

PROPOSED SYSTEM:

- This document presents a new move toward for user verification and session organization that is applied in the situation aware security by

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

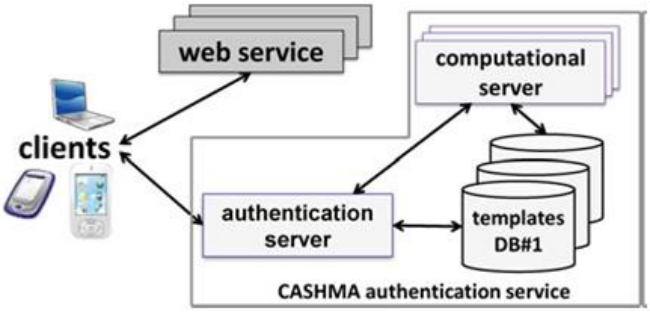
hierarchical multilevel architectures (CASHMA) system for secure biometric authentication on the Internet.

- CASHMA is able to operate strongly with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices, e.g., smart phones, Desktop PCs or even biometric kiosks placed at the opening of secure areas. Depending on the preference and requirements of the owner of the web examine, the CASHMA authentication examination can complement a traditional authentication service, or can replace it.
- Our unbroken authentication move toward is grounded on transparent acquisition of biometric information and on adaptive timeout organization on the foundation of the trust posed in the user and in the different subsystems used for verification. The user meeting is open and secure despite potential idle activity of the user, while possible misuses are detected by always confirming the attendance of the good user.

ADVANTAGES OF PROPOSED SYSTEM:

- Our move toward does not need that the response to a consumer confirmation mismatch is executed by the user device (e.g., the logout procedure), other than it is clearly handled by the CASHMA authentication service and the web services, which be relevant their own response procedures.
- Provides a exchange between usability and safety.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

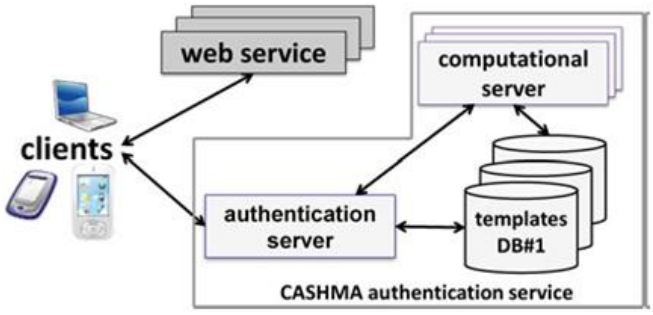
HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE
- IDE : Netbeans 7.4
- Database : MYSQL

SYSTEM ARCHITECTURE:



IMPLEMENTATION:

MODULES:

- System Model
- Authentication Server
- CASHMA Certificate
- Continuous Authentication

MODULES DESCRIPTION:

System Model:

- ✓ In this module, we create the System model to evaluate and implement our proposed system. CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA authentication service by discussing the sample application scenario, where a user u wants to log into an online banking service.

- ✓ "User Id" refers to the identity of the user obtained from the Bank for the purpose of logging into the Internet Banking facility provided by the Bank.
- ✓ "Login Password" is a unique and randomly generated password known only to the customer, which can be changed by the user to his/her convenience. This is a means of authenticating the user ID for logging into Internet Banking.
- ✓ "Transaction Password" is a unique and randomly generated password known only to the customer, which can be changed to his/her convenience. This is a means of authentication required to be provided by the customer for putting through the transaction in his/her/their/its accounts with Bank through Internet Banking. While User ID and Password are for valid access into the internet application, giving valid Transaction Password is for authentication of transaction/requests made through internet.

Authentication Server:

- ✓ In Internet banking as with traditional banking methods, security is a primary concern. Server will take every precaution necessary to be sure your information is transmitted safely and securely. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the system.
- ✓ The Server maintains the functionality:
  - Customer Details
  - Activation of Beneficiary
  - Transaction Details
  - Activate Blocked Account

CASHMA Certificate:

- ✓ In this module, we present the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol. Time stamp and sequence number univocally identify each certificate, and protect from replay attacks. ID is the user ID, e.g., a number.
- ✓ Decision represents the outcome of the verification procedure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. In fact, the global trust level and the session timeout are always computed considering the time instant in which the CASHMA application acquires the biometric data, to avoid potential problems related to unknown delays in communication and computation.

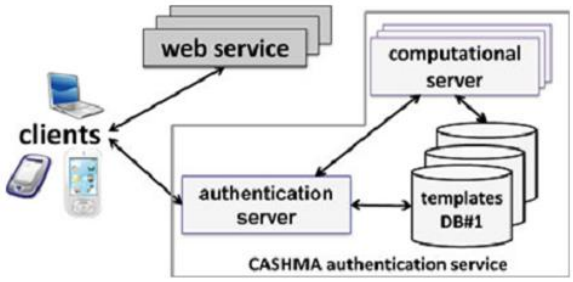
Continuous Authentication:

- ✓ 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 use of biometric authentication allows credentials to be acquired transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability.
- ✓ The idea behind the execution of the protocol is that the client continuously and transparently acquires and transmits evidence of the user identity to maintain access to a web service. The main task of the proposed protocol is to create and then maintain the user session adjusting the session timeout on the basis of the confidence that the identity of the user in the system is genuine.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

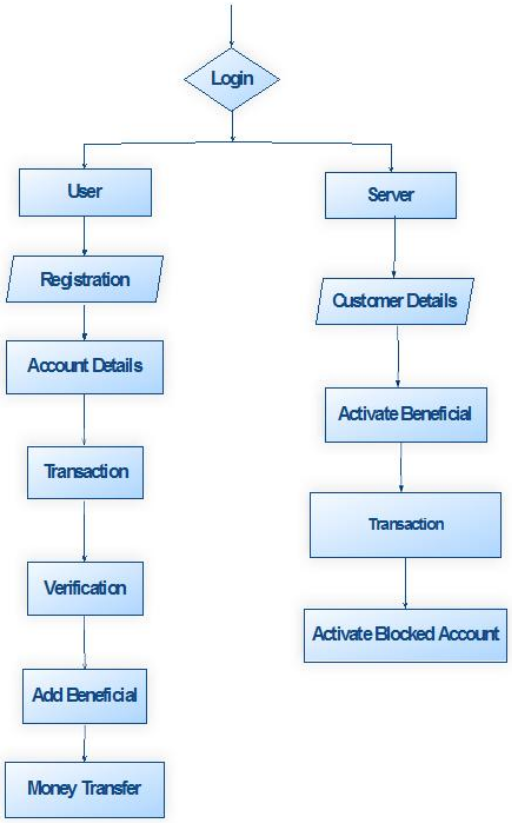
SYSTEM DESIGN:

SYSTEM ARCHITECTURE:



DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



UML DIAGRAMS:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The UML uses mostly graphical notations to express the design of software projects.

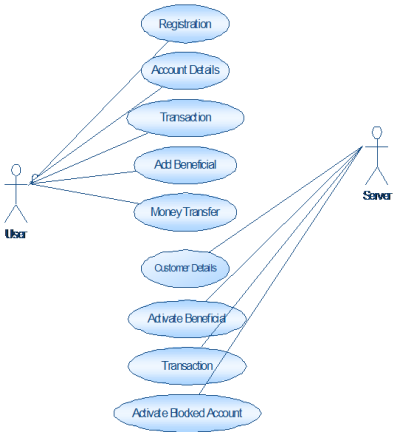
GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

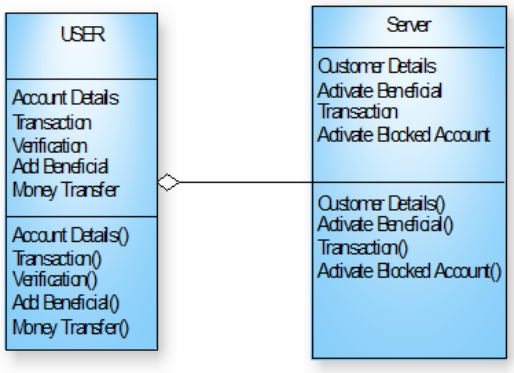
USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



CLASS DIAGRAM:

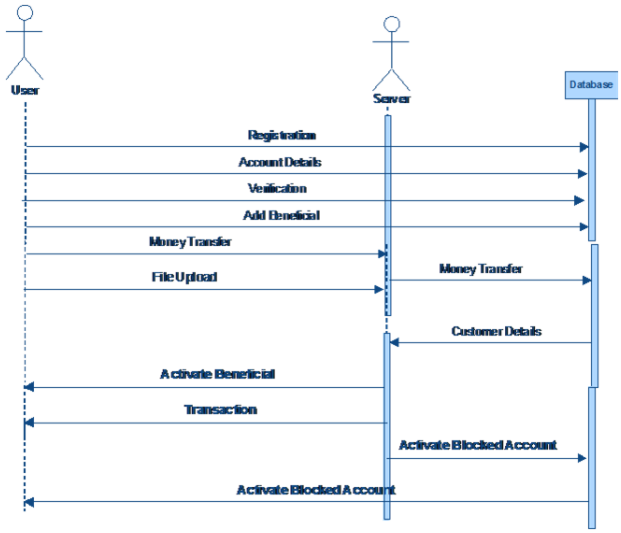
In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order.

It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

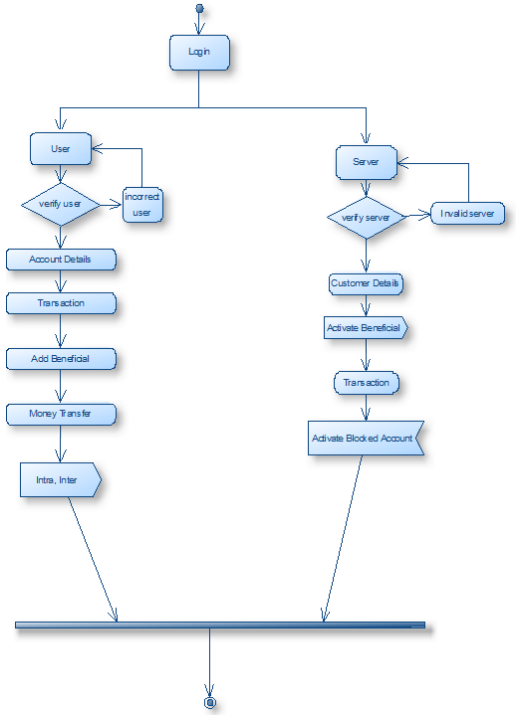


ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



LITERATURE SURVEY

1) Quantitative Security Evaluation of a Multi-Biometric Authentication System

AUTHORS: L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,

Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures. In this paper we perform a quantitative security evaluation of the CASHMA multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVISE modeling formalism, a formalism for security evaluation that extends attack graphs; it allows to combine information on the system, the attacker, and the metrics of interest to produce quantitative results. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios.

2) Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform

AUTHORS: L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and
A. Bondavalli

Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security issues to be faced arise from exposing applications and data to the Internet, thus requiring an attentive analysis of potential threats and the identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance and scalability properties. The paper presents a model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform, by evaluating how the introduction of security mechanisms may lead to a degradation of performance properties. The evaluation focuses on the OPENNESS platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model, and the evaluation of different configuration by composing them in different ways.

3) Attacks on Biometric Systems: A Case Study in Fingerprints

AUTHORS: U. Uludag and A.K. Jain

In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. In this paper, we analyze these attacks in the realm of a fingerprint biometric system. We propose an attack system that uses a hill climbing procedure to synthesize the target minutia templates and evaluate its feasibility with extensive experimental results conducted on a large fingerprint database. Several measures that can be utilized to decrease the probability of such attacks and their ramifications are also presented.

4) Automated Generation and Analysis of Attack Graphs

AUTHORS: O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing

An integral part of modeling the global view of network security is constructing attack graphs. Manual attack graph construction is tedious, error-prone, and impractical for attack graphs larger than a hundred nodes. In this paper we present an automated technique for generating and analyzing attack graphs. We base our technique on symbolic model checking algorithms, letting us construct attack graphs automatically and efficiently. We also describe two analyses to help decide which attacks would be most cost-effective to guard against. We implemented our technique in a tool suite and tested it on a small network example, which includes models of a firewall and an intrusion detection system.

5) Risk-Based Security Engineering through the Eyes of the Adversary

AUTHORS: S. Evans and J. Wallner

Today, security engineering for complex systems is typically done as an ad hoc process. Taking a risk-based security engineering approach replaces today's ad hoc methods with a more rigorous and disciplined approach that uses a multi-criterion decision model. This approach builds on existing techniques for integrating risk analysis with classical systems engineering. A resulting security metric can be compared with cost and performance metrics in making engineering trade-off decisions.

CONCLUSION:

We broken the original option introduce by biometrics to define a procedure for uninterrupted verification that improve security and usability of user meeting. The protocol compute adaptive timeouts on the basis of the trust posed in the user activity and in the excellence and kind of biometric data acquire transparently through monitor in background the user's events. Some architectural design decision of CASHMA are here discuss. First, the system interactions raw information and not the features extracted from them or templates, while cripto-token approaches are not considered; as debated in Section 3.1, this is due to architectural decision where the customer is kept very easy. We remark that our future protocol works with no change using features, template or raw information. Second, privacy concern must be address consider National legislations. At near, our prototype only perform some check on face detection, where single one face (the biggest single rust from the face discovery.

REFERENCES:

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

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[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 (SCS '08), pp. 1-6, Nov. 2008.

[4] BioID "Biometric Authentication as a Service (BaaS)," BioID 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.

[6] 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.

[7] 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.

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

[9] C. Roberts, "Biometric Attack Vectors and Defences," Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.

[10] S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. first ed., Springer, 2009.

[11] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633, 2004.

[12] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W.H. Sanders, "Adversary-Driven State-Based System Security Evaluation," Proc. the Sixth Int'l Workshop Security Measurements and Metrics (MetriSec '10), pp. 5:1-5:9, 2010.

[13] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing , "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.

[14] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evaluation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

[15] T. Courtney, S. Gaonkar, L. Keefe, E.W.D. Rozier, and W.H. Sanders, "M€obius 2.3: An Extensible Tool for Dependability, Security, and Performance Evaluation of Large and Complex System Models," Proc. IEEE/IFIP Int'l Conf. Dependable Systems & Networks (DSN '09), pp. 353-358, 2009.

[16] W.H. Sanders and J.F. Meyer, "Stochastic Activity Networks: Formal Definitions and Concepts," Lectures on Formal Methods and Performance Analysis, pp. 315-343, Springer-Verlag, 2002.

[17] T. Casey, "Threat Agent Library Helps Identify Information Security Risks,," White Paper, Intel Corporation, Sept. 2007.

[18] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, "Improving Security of Internet Services through Continuous and Transparent User Identity Verification," Proc. Int'l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[19] Adobe Products List, http://www.adobe.com/products, 2014.

[20] T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,," Banking & Technology Snapshot, DB Research, Feb. 2012.

[21] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.

[22] L. Allano, B. Dorizzi, and S. Garcia-Salicetti, "Tuning Cost and Performance in Multi-Biometric Systems: A Novel and Consistent View of Fusion Strategies Based on the Sequential Probability Ratio Test (SPRT)," Pattern Recognition Letters, vol. 31, no. 9, pp. 884-890, 2010.

[23] S. Evans and J. Wallner, "Risk-Based Security Engineering through the Eyes of the Adversary," Proc. the IEEE Workshop Information Assurance, pp. 158-165, June 2005.

[24] M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, and L. Romano, "A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures," Proc. Int'l Symp. High-Assurance Systems Eng. (HASE), pp. 48-55, 2012.

[25] M. Cinque, D. Cotroneo, R. Natella, and A. Pecchia, "Assessing and Improving the Effectiveness of Logs for the Analysis of Software faults," Proc. Int'l Conf. Dependable Systems and Networks (DSN), pp. 457-466, 2010.

[26] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, and H. Madeira, "Assessing and Comparing Security of Web Servers," Proc. IEEE Int'l Symp. Dependable Computing (PRDC), pp. 313-322, 2008.

[27] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli, "Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform," Electronic.

Author's Details:

Jadi Vasantha
Assistant Professor, Department of CSE,
VIF College of Engineering and Technology.