A Novel Secure Protocol for Continuous Authentication using Blowfish Algorithm

YALLA TEJASWINI [#1] and D.VIJAYA KUMARI [*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology, Department of Computer Science and Engineering, JNTUK, A.P, India.*

[*] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA*

***Abstract*— The paper presents an enhanced CASHMA architecture. The existing works exploited the novel possibility introduced by the biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background of user's actions. But there is a lack of security in the Biometric Templates. To overcome this drawback Blowfish algorithm is used for encryption and decryption and it provides more security. Blowfish algorithm works on variable key length. It works on bit length ranges from 64-448 because of which it takes less execution time. The objective of blowfish algorithm is to encrypt the data in a short execution time with minimum cost. The biometric templates are encrypted which are all converted from the multimedia file before transferring to the buyer. It improves the efficiency of the process.**

***Index Terms*— Security, Web servers, Authentication, Mobile Environments.**

I. Introduction

Session management for Internet services are traditionally based on username and password, and sessions are terminated by explicit logouts or by the expiration of session timeouts. One single verification point is applied but may be deemed insufficient or not satisfactory as the identity of a user is considered immutable during the entire session. Continuously authenticating internet users has become a significant priority because, there has been a tremendous surge in the amount of personal data and sensitive information stored or accessed [1]. Login-time pins and textual and graphical passwords are by far the most popular mechanisms for authenticating the users.

However, these mechanisms suffer from at least two drawbacks: (1) they are static, i.e., they authenticate the user once – at the beginning of a session – and do not offer any protection against unauthorized access post login; and (2) passwords and pins require user's attention for their entry and therefore are not suitable for continuous authentication. Hence biometrics was used to define a protocol for continuous authentication that improves security and usability of a user session [2].

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 authentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors [3].

Implicit or "active" authentication is an emerging area in smart phone domain, which aims to continuously authenticate users without interrupting them. There is also growing evidence that users tend to choose simple text and graphical passwords, making them relatively easy to guess formed by harnessing the users' natural interactions with the smart phone [4]. Lately, behavioural modalities that have been used for active authentication include on-screen touch and gestures, hand or smart phone movement and orientation, geo-location patterns and combinations of these. Among the aforementioned modalities for active authentication of smart phone users, touch has been gaining popularity because: (1) there is growing evidence that touch patterns can be used to create reliable signatures for user authentication, and (2) most interactions with smart phone applications happen as taps, touch strokes and gestures, so these patterns are easily available for enrolment and subsequent authentication [5].

A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials again and again. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal bio-metric continuous authentication are proposed, turning user verification into a continuous process instead of onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits, new approach for user's verification and session management are discussed in this paper that is defined and implemented in the context of the multi-modal biometric authentication system CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture). The CASHMA system realizes a secure biometric authentication service on the Internet, in this users need to remember only one username and use their biometric data rather than passwords to authenticate in multiple web services. CASHMA operate securely with any kind of web service for example online banking, military zones, and airport zone which require high security services [6].

II. LITERATURE SURVEY

Bondavalli, et al., [7] presented a Biometric authentication system to 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.

Montecchi, et al., [8] showed that 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 evaluations aim 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. 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.

Uludag et al., [9] showed that, 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.

Sheyner et al., [10] presented 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.

S. Evans and J. Wallner [11] showed that 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.

III. EXISTING SYSTEM

The existing protocol requires a sequential multi-modal biometric system composed of n modal biometric subsystems that are able to decide independently on the authenticity of a user. 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 assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session. In existing, a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The work in another existing paper, proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on the type of biometric traits and time, since different sensors are able to provide raw data with different timings. A time constraint introduces the need of a temporal integration method which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function [13, 14].

A. *DISADVANTAGES OF EXISTING SYSTEM*

1. None of existing approaches supports continuous authentication [1, 17].
2. Emerging biometric solutions allow substituting username and password with biometric data during 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.

IV. PROPOSED SYSTEM

This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) system 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, and it is intended to be used from different client devices, e.g., smart phones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it. Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication. The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.

A. *ADVANTAGES OF PROPOSED SYSTEM*

- Our approach does not require that the reaction to a user verification mismatch is executed by the user device (e.g., the logout procedure), but it is transparently handled by the CASHMA authentication service and the web services, which apply their own reaction procedures.
- Provides a tradeoff between usability and security.

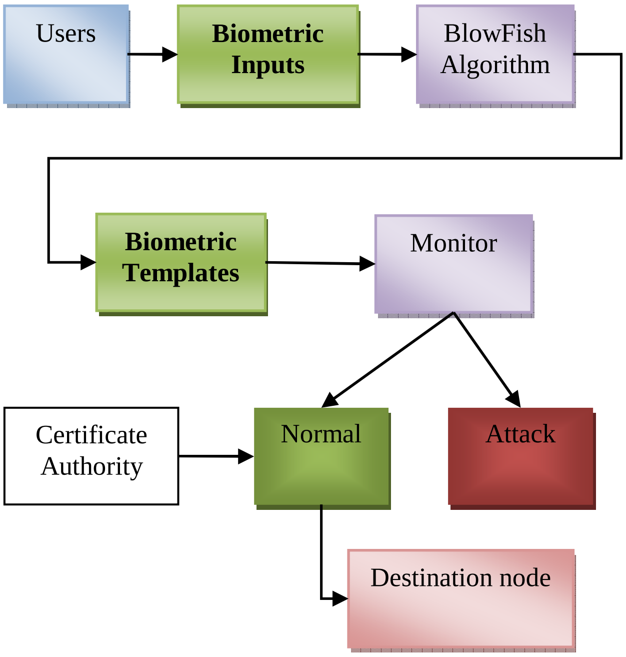


Fig.1 Block Diagram

B. *SYSTEM MODEL*

The user (the client) communicates with the web service for a service request; the web service replies a valid certificate from the CASHMA authentication service is required for authentication. The first step is sending the data for the different biometric traits, specifically selected to perform a strong authentication procedure. The CASHMA authentication server checks the biometric data received and performs an authentication procedure. There are two different possibilities arises. If the user identity is not verified, new or additional biometric information are requested (back to step 1); this process is repeated until the minimum trust threshold is reached. If the user identity is successfully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length T1 at time instant timestamp1 for the user session. Creates the CASHMA certificate and sends it to the client. - The client forwards the CASHMA certificate to the web service. The certificate is read by web server and authorizes the client to use the requested service until time timestamp.

The web service demands the authentication of users to the CASHMA authentication server. These services are any kind of Internet service. Finally, by clients we mean the users' devices like (laptops, Desktop PCs, tablets, etc.) which acquire the biometric data corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server towards a target web service. A client contains .i) sensors - acquire the raw data, ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA authentication server applies user authentication and verification procedures that compare the raw data with the biometric templates stored.

C. *AUTHENTICATION PROTOCOL*

In the following we have given the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, which is necessary to understand details of the protocol. Time stamp and sequence number identify each certificate, and protect from replay attacks. the outcome of the verification is decision ,carried out on the server side. It consists of the expiration time of the session that is assigned by the CASHMA authentication server. The global trust level and the session timeout are usually computed considering the time instant in which the CASHMA application acquires the biometric data.

V. IMPLEMENTATION

The proposed system of this paper is divided into four major modules and described as below.

1. System Model
2. Authentication Server
3. CASHMA Certificate
4. Continuous Authentication

A. *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 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.

B. *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:

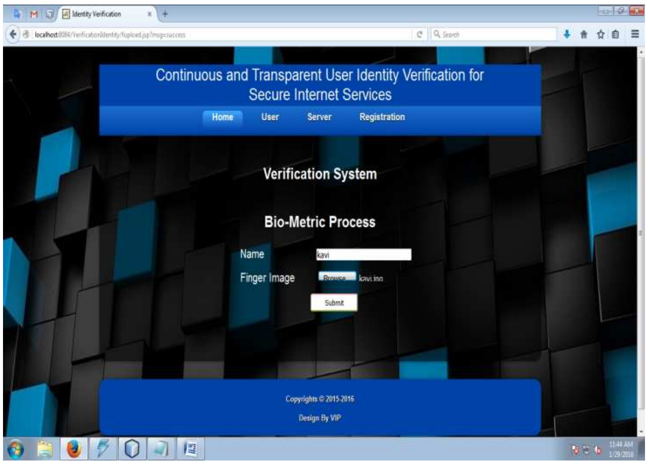
- Customer Details
- Activation of Beneficiary
- Transaction Details
- Activate Blocked Account

C. *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. 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.

D. *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.



Continuous and Transparent User Identity Verification for Secure Internet Services

Verification System

Bio-Metric Process

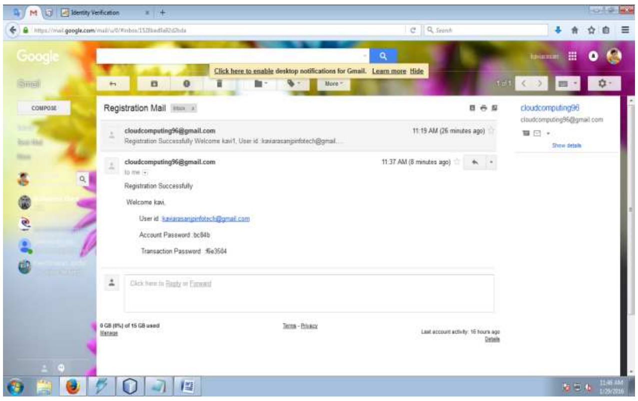
Name: kavi

Finger Image: kavi.jpg

Copyrights © 2015-2016

Design By VIP

Fig.2 Registration form



Registration Mail

cloudcomputing96@gmail.com 11:19 AM (26 minutes ago)
Registration Successfully Welcome kavi1, User id :kaviarasanjpinfotech@gmail...

cloudcomputing96@gmail.com 11:37 AM (8 minutes ago)
to me

Registration Successfully

Welcome kavi,

User id: kaviarasanjpinfotech@gmail.com

Account Password :bc84b

Transaction Password :f6e3504

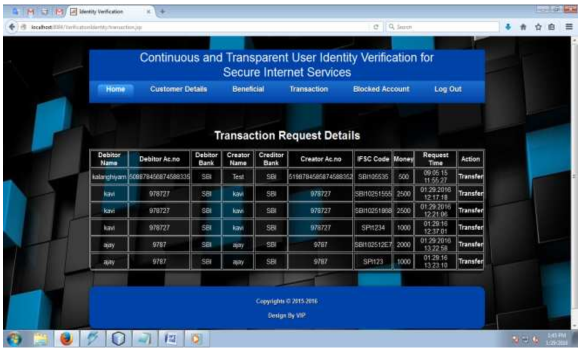
Click here to Reply or Forward

0 GB (0%) of 15 GB used

Last account activity: 16 hours ago

Identity Verification
https://mail.google.com/mail/u/0/#inbox/152fbedfa82d2bda
Google
Gmail
Click here to enable desktop notifications for Gmail. Learn more Hide
More
COMPOSE
Inbox
1 of 1
cloudcomputing96
cloudcomputing96@gmail.com
Show details
Manage
Terms - Privacy
Details
11:46 AM
1/29/2016

Fig.3 Registration Confirmation Mail with A/c password & transaction password

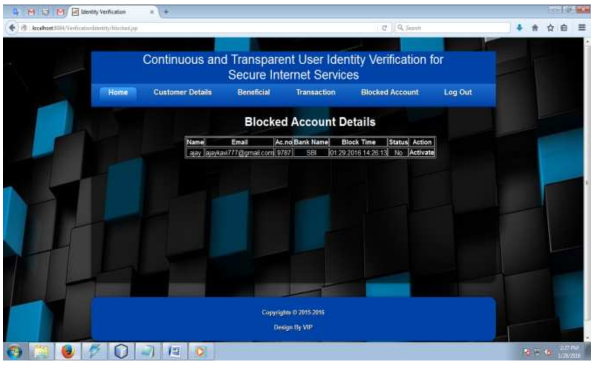


Transaction Request Details

Debitor Name	Debitor Ac.no	Debitor Bank	Creator Name	Creditor Bank	Creator Ac.no	IFSC Code	Money	Request Time	Action
kalanghiyam	5088784568745888335	SBI	Test	SBI	5198784585874588352	SBI105535	500	09:05:15 11:55:27	Transfer
kavi	978727	SBI	kavi	SBI	978727	SBI10251555	2500	01:29:2016 12:17:18	Transfer
kavi	978727	SBI	kavi	SBI	978727	SBI10251868	2500	01:29:2016 12:21:06	Transfer
kavi	978727	SBI	kavi	SBI	978727	SPI1234	1000	01:29:16 12:37:01	Transfer
ajay	9787	SBI	ajay	SBI	9787	SBI102512E7	2000	01:29:2016 13:22:58	Transfer
ajay	9787	SBI	ajay	SBI	9787	SPI123	1000	01:29:16 13:23:10	Transfer

Copyrights © 2015-2016
Design By VIP

Fig.4 Transaction Request Details



Blocked Account Details

Name	Email	Ac.no	Bank Name	Block Time	Status	Action
ajay	ajaykavi777@gmail.com	9787	SBI	01:29:2016 14:26:13	No	Activate

Copyrights © 2015-2016
Design By VIP

Fig.5 Blocked Account Details

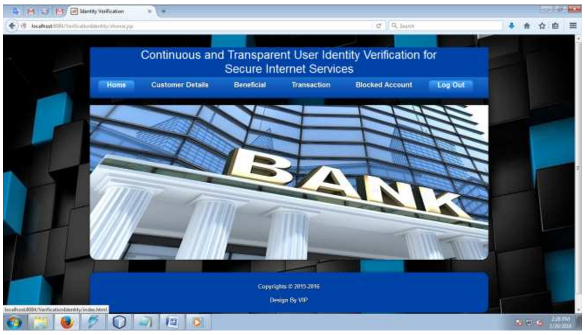


Fig.6 Server Logout

VI. CONCLUSION

Session management system is fully based on username and password, and sessions are terminated by explicit logouts or by the expiration of session timeouts. One single verification point is applied but may be seem not sufficient or not satisfactory because the identity of a user is supposed immutable during the entire session. This paper presents a protocol for continuous authentication which improves security and usability of a user session. The protocol computes adaptive timeouts which is based on the trust put on the activity of user and in the quality as well as the kind of biometric data user is providing. The transparent acquisition of biometric data, realized through monitoring in background the user's actions, allows maintaining the session open without explicit interactions with the user, thus improving usability.

The proposed protocol performs only some checks on face recognition, where only one face is considered for identity verification and the others deleted. Also when data is acquired in an uncontrolled environment, the quality of biometric data could strongly depend on the surroundings. Our future work will be set to eradicate these limitations.

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 (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.

[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] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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 PROFILE

YALLA TEJASWINI

is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science & Engineering).Her Area of interest includes Secure Computing and its objectives in all current trends and techniques in Computer Science.

D.VIJAYA KUMARI M.TECH

is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute Of Engineering & Technology affiliated to JNTUK. A.P, India.