AN ADVANCED AND TRANSPARENT SECURITY MODEL FOR USER AUTHENTICATION IN INTERNET SERVICES

K. Sravanthi,

Dept. of MCA, QIS college of Engineering and Technology, Ongole

Abstract: In distributed Internet Services the session management is achieved based on username and password, explicit logouts and systems of client session expiration using great timeouts. Developing biometric arrangements permit substituting username and password with biometric information amid session foundation, yet in such a methodology still a solitary check is esteemed adequate, and the character of a client is viewed as changeless amid the whole session. Also, the length of the session timeout may affect on the ease of use of the administration and subsequent customer fulfillment. This paper investigates promising options offered by applying biometrics in the administration of sessions. A protected convention is characterized for interminable validation through nonstop client confirmation. The convention decides versatile timeouts dependent on the quality, recurrence and kind of biometric information straightforwardly gained from the client. The practical conduct of the convention is outlined through Matlab reproductions, while display based quantitative investigation is completed to evaluate the capacity of the convention to differentiate security assaults practiced by various types of assailants. At long last, the present model for PCs and Android cell phones is examined.

Keywords: *Administration, Security, Authentication, Mobile environment.*

I. INTRODUCTION

Secure client verification is major in the vast majority of current ICT frameworks. Client confirmation frameworks are customarily dependent on sets of username and secret key and confirm the character of the client just at login stage. No checks are performed amid working sessions [1], which are ended by an express logout or lapse after an inactive movement time of the client [2]. Security of online applications is a genuine concern, because of the ongoing increment in the recurrence and multifaceted nature of digital assaults [3]; biometric systems [10] offer developing answer for secure and confided in validation, where username what's more, secret word are supplanted by biometric information. In any case, parallel to the spreading use of biometric frameworks, the motivator in their abuse is additionally developing [4], particularly considering their conceivable application in the money related and banking segments [20], [11].

Such perceptions lead to belligerence that a solitary verification point and a solitary biometric information can't ensure a adequate level of security [5][6][7]. Indeed, comparably to customary verification forms which depend on username what's more, secret key, biometric client validation is ordinarily figured as a "solitary shot" [8], giving client check just amid login stage when at least one biometric attributes might be required. When the client's character has been checked, the framework assets are accessible for a fixed timeframe or on the other hand until unequivocal logout from the client. This methodology expect[9], that a solitary confirmation (toward the start of the session) is adequate, and that the character of the client is consistent amid the entire session. For example, we consider this basic situation: a client has just signed into a security- basic administration, and after that the client leaves the PC unattended in the work zone for some time. This issue is even trickier with regards to cell phones, regularly utilized in broad daylight what's more, swarmed situations, where the gadget itself can be lost or persuasively stolen while the client session is dynamic, permitting impostors to imitate the client and access entirely individual information. In these situations, the administrations where the clients are verified can be abused effectively [8], [5]. A essential arrangement is to utilize exceptionally short session timeouts and intermittently ask for the client to enter his/her certifications over furthermore, finished, however this is certainly not an authoritative arrangement and intensely punishes the administration ease of use and at last the fulfillment of clients [12][13]. To auspicious recognize abuses of PC assets and forestall that an unapproved client noxiously replaces an approved one, arrangements dependent on multi-modular biometric nonstop confirmation [5] are proposed, turning client check into a nonstop procedure instead of an onetime event [8]. To maintain a strategic distance from that a solitary biometric quality is manufactured, biometrics confirmation can depend on different biometrics attributes [14]. At last, the utilization of biometric validation enables accreditations to be procured straightforwardly, i.e., without unequivocally telling the client or requiring his/her connection, which is basic to ensure better administration [15], convenience. We present a few instances of straightforward securing of biometric information. Face can be obtained while the client is situated in front of the camera, however not deliberately for the procurement of the biometric information; e.g., the client might peruse a literary SMS or viewing a motion picture on the cell phone. Voice can be obtained when the client talks on the telephone [16], or with other individuals close-by if the receiver dependably catches foundation. Keystroke information can be procured at whatever point the client types on the console, for instance, when composing an SMS, visiting, or perusing on the Internet [17]. This methodology separates from conventional verification forms, where username/secret word are asked for just once at login time or unequivocally required at affirmation steps; such customary confirmation approaches hinder ease of use for improved security, and offer no arrangements against falsification or taking of passwords [18].

II RELATED WORK

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

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 [19]; 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 [20], provided by different system configurations against attackers with different capabilities [21]. The analysis is performed using the ADVICE modeling formalism, a formalism for security evaluation that extends attack graphs; it allows combining 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.

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

Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability [22]. 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 [23], 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 [24], 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 [25]. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability [26]. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model [27], and the evaluation of different configuration by composing them in different ways.

III. EXISTING SYSTEM

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 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 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.

Disadvantages:

- None of existing approaches supports continuous authentication.
- 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.

Advantages:

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.

V. THE CONTINUAL AUTHENTICATION PROTOCOL

The continuous authentication protocol permits providing adaptive session timeouts to an internet service to line up and maintain a secure session with a shopper. The timeout is adapted on the premise of the trust that the CASHMA authentication system puts within the biometric subsystems and within the user. Details on the mechanisms to cipher the adaptative session timeout square measure.

Description of the Protocol

The projected protocol needs a ordered multi-modal biometric system composed of n unimodal biometric subsystems that square measure able to decide severally on the authenticity of a user. for instance, these subsystems will be one scheme for keystroke recognition and one for face recognition.

The idea behind the execution of the protocol is that the client ceaselessly and transparently acquires and transmits evidence of the user identity to keep up access to a web service. The most task of the projected protocol is to create so maintain the user session adjusting the session timeout on the premise of the boldness that the identity of the user within the system is real. The execution of the protocol consists of consecutive phases: the initial part and therefore the maintenance part. The initial part aims to demonstrate the user into the system and establish the session with the online service. During the maintenance part, the session timeout is adaptively updated when user biometric authentication is performed victimization contemporary raw data provided by the shopper to the CASHMA authentication server. These phases square measure elaborate hereafter with the help of Initial part. This part is structured as follows: The user (the client) contacts the online service for a service request; the online service replies that a legitimate certificate from the CASHMA authentication service is needed for authentication. victimization the CASHMA application, the shopper contacts the CASHMA authentication server. the primary step consists in deed and causation at time t0 the information for the various biometric traits, specifically chosen to perform a robust authentication procedure.

The application expressly indicates to the user the biometric traits to be provided and doable retries. The CASHMA authentication server analyzes the biometric knowledge received associated performs an authentication procedure. Completely different prospects arise here. If the user identity isn't verified (the world trust level is below the trust threshold gmin), new or further biometric knowledge square measure requested till the minimum trust threshold gmin is reached. Instead if the user identity is with success verified, the CASHMA authentication server authenticates the user, computes associate initial timeout of length T0 for the user session, set the expiration time at T0 þ t0, creates the CASHMA certificate and sends it to the shopper.

The shopper forwards the CASHMA certificate to the web service coupling it with its request. The online service reads the certificate and authorizes the shopper to use the requested service (step 4) till time t0 þ T0. For clarity, square measures diagrammatic in Fig. three for the case of prosperous user verification solely. Maintenance part. It’s composed of 3 steps perennial iteratively: once at time ti the shopper application acquires contemporary (new) data (corresponding to 1 biometric trait), it communicates them to the CASHMA authentication server. The biometric knowledge will be acquired transparently to the user; the user might but decide to give biometric knowledge that square measure unlikely nonheritable in an exceedingly clear manner. Finally once the session timeout goes to expire, the shopper might expressly give notice to the user that fresh biometric knowledge square measure required.

The CASHMA authentication server receives the biometric data from the shopper and verifies the identity of the user. If verification isn't prosperous, the user is marked as not legitimate, and consequently the CASHMA authentication server doesn't operate to refresh the session timeout. This doesn't imply that the user is cut-off from this session: if alternative biometric knowledge square measure provided before the timeout expires, it's still doable to induce a replacement certificate and refresh the timeout. If verification is prosperous, the CASHMA authentication server applies the rule detailed in Section four.2 to adaptively cipher a new timeout of length Ti, the expiration time of the session at time Ti þ ti so it creates and sends a new certificate to the shopper.

The shopper receives the certificate and forwards it to the web service; the online service reads the certificate Initial introduce case of prosperous user authentication. Maintenance introduce case of prosperous user verification.

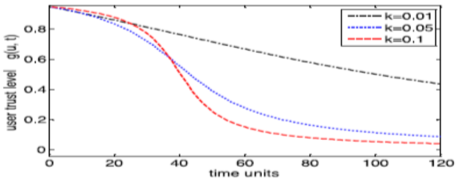
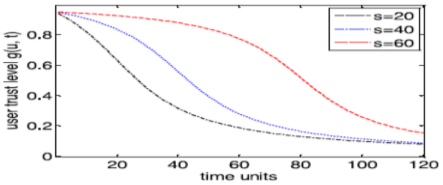


Fig. 5. Evolution of the user trust level when $k = [0.01, 0.05, 0.1]$ and $s = 40$.



5. Evolution of the user trust level when $k = 0.05$ and $s = [20, 40, 60]$.

The steps of the upkeep part square measure diagrammatic.

VI. SYSTEM ARCHITECTURE

The overall system is composed of the CASHMA authentication service, the clients and the web services (Fig.), connected through communication channels. Each communication channel in Fig. implements specific security measures which are not discussed here for brevity. The CASHMA authentication service includes: i) an authentication server, which interacts with the clients, ii) a set of high-performing computational servers that perform com-parisons of biometric data for verification of the enrolled users, and iii) databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification). The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled users to the CASHMA authentication server. These services are poten-tially any kind of Internet service or application with requirements on user authenticity. They have to be regis-tered to the CASHMA authentication service, expressing also their trust threshold. If the web services adopt the continuous authentication protocol, during the registration process they shall agree with the CASHMA registration office on values for parameters h; k and s used.

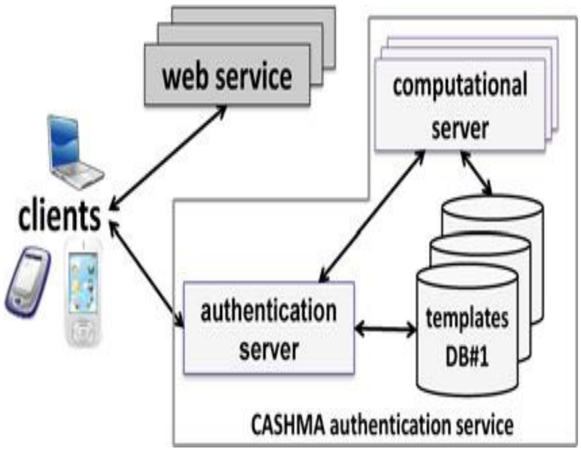


Fig: CASHMA Architecture

Finally, by clients we mean the users' devices (laptop and desktop PCs, smartphones, tablet, etc.) that acquire the bio-metric data (the raw data) corresponding to the various bio-metric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentica-tion procedure towards the target web service. A client con-tains i) sensors to acquire the raw data, and ii) the CASHMA application which transmits the biometric data to the authentication server. The CASHMA authentication server exploits such data to apply user authentication and successive verification procedures that compare the raw data with the stored biometric templates.

Transmitting raw data has been a design decision applied to the CASHMA system, to reduce to a minimum the dimension, intrusiveness and complexity of the applica-tion installed on the client device, although we are aware that the transmission of raw data may be restricted, for example, due to National legislations.

CASHMA includes countermeasures to protect the bio-metric data and to guarantee users' privacy, including poli-cies and procedures for proper registration; protection of the acquired data during its transmission to the authentica-tion and computational servers and its storage; robustness improvement of the algorithm for biometric verification Privacy issues still exist due to the acquisition of data from the surrounding environment as, for example, voices of people nearby the CASHMA user, but are considered out of scope for this paper.

The continuous authentication protocol explored in this paper is independent from the selected architectural choices and can work with no differences if templates and feature sets are used instead of transmitting raw data, or indepen-dently from the set of adopted countermeasures.

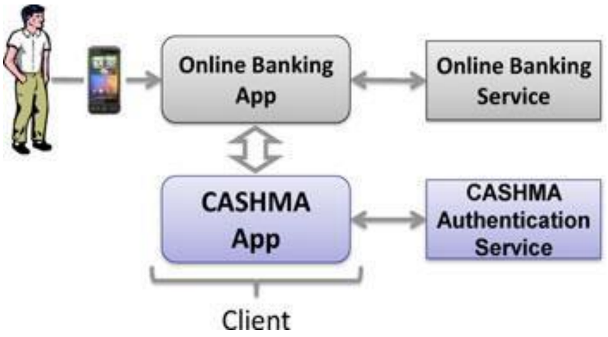
Sample Application Scenario

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 in Fig. where a user u wants to log into an online banking service using a smartphone.

It is required that the user and the web service are enrolled to the CASHMA authentication service. We assume that the user is using a smartphone where a CASHMA application is installed.

The smartphone contacts the online banking service, which replies requesting the client to contact the CASHMA authentication server and get an authentication certificate. Using the CASHMA application, the smartphone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the user identity, and grants the access if: i) it is enrolled in the CASHMA authentication service, ii) it has rights to access the online banking service and, iii) the acquired biometric data match those stored in the templates database associ-ated to the provided identifier. In case of successful user verification, the CASHMA authentication server releases an authentication certificate to the client, proving its identity to third parties, and includes a timeout that sets the maximum duration of the user session. The client presents this certifi-cate to the web service, which verifies it and grants access to the client.

The CASHMA application operates to continuously maintain the session open: it transparently acquires biomet-ric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certifi-cate, which includes a new timeout, is forwarded to the web service to further extend the user session.



Example scenario: accessing an online banking service using a smart phone

The System Components are given below

System Model:

In this entity, 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.

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.

Customer Details:

A multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The proposed approach assumes that first the user logs in using a strong authentication procedure, then a continuous verification process is started based on multi-modal biometric. Verification failure together with a conservative estimate of the time required to subvert the computer can automatically lock it up. Similarly, a multi-modal biometric verification system is presented, which continuously verifies the presence of a user working with a computer. If the verification fails, the system reacts by locking the computer and by delaying or freezing the user's processes.

Activation of Beneficiary:

Beneficiary Details Added by the customer who want to do the third party transaction beneficiary type is 1) intra account 2)inter account type after the process ,beneficiary is activated by the admin.

CASHMA Certificate

In this entity, 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.

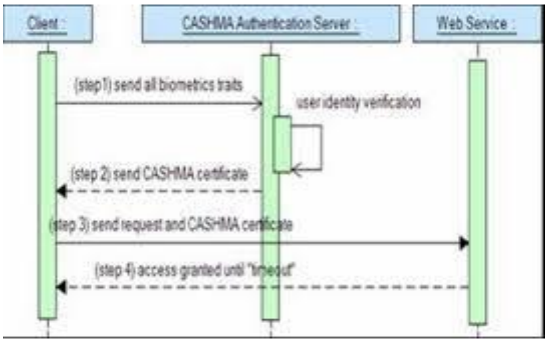

Client :
CASHMA Authentication Server :
Web Service :
(step1) send all biometrics traits
user identity verification
(step 2) send CASHMA certificate
(step 3) send request and CASHMA certificate
(step 4) access granted until "timeout"

Fig: Initial Phase in case of Successful user authentication

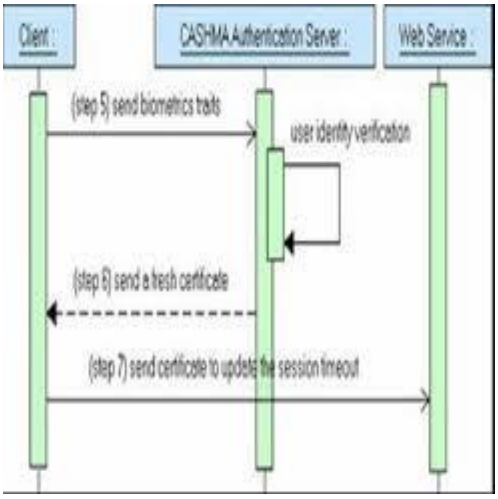

Client :
CASHMA Authentication Server :
Web Service :
(step 5) send biometrics traits
user identity verification
(step 6) send a fresh certificate
(step 7) send certificate to update the session timeout

Fig. Maintenance phase in case of successful user verification

VII. RESULT

This paper provides various existing methods used for continuous authentication using different biometrics. Initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

VIII. CONCLUSION

In this paper, we expressed the novel probability presented by biometrics to characterize a convention for ceaseless verification that improves security and convenience of client session. The protocol computes versatile timeouts based on the trust posed in the client movement and in the quality and sort of biometric data obtained straightforwardly through checking in background the client's actions. Some structural plan choices of CASHMA are here talked about. Initially, the framework trades crude information and not the highlights separated from them or formats, while cripto-token methodologies are not considered, this is because of building choices where the client is kept extremely straightforward. We comment that our proposed protocol works without any progressions utilizing highlights, templates or crude information. Second, security concerns ought to be addressed considering National enactments. At present, our prototype only plays out certain minds face acknowledgment, where only one face (the greatest one rusting from the face identification).

IX. REFERENCES

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

[2] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics ImprovePerformance?" Proc. Workshop on Automatic Identification AdvancesTechnologies (AutoID '99) Summit, pp. 59-64, 1999.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable AuthenticationDevice 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 PressRelease, https://www.bioid.com, Mar. 2011.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "ContinuousVerification Using Multimodal Biometrics," IEEE Trans. PatternAnalysis 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 AuthenticationSystem," Proc. Int'l Conf. Computer Safety, Reliability andSecurity, pp. 209-221, 2012.

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using ContinuousBiometric 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 ContinuousMultimodal 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 CaseStudy in Fingerprints," Proc. SPIE-EI 2004, Security, Steganographyand Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633,2004.

[12] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, andW.H. Sanders, "Adversary-Driven State-Based System SecurityEvaluation," Proc. the Sixth Int'l Workshop Security Measurementsand 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. Dependableand 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 ComplexSystem 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: FormalDefinitions and Concepts," Lectures on Formal Methods and PerformanceAnalysis, pp. 315-343, Springer-Verlag, 2002.

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

[18] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina,"Improving Security of Internet Services through Continuous andTransparent User Identity Verification," Proc. Int'l Symp. ReliableDistributed 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: BiometricsEnjoy Remarkable Degree of Acceptance,," Banking &Technology Snapshot, DB Research, Feb. 2012.

[21] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for InformationSecurity," 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 andPerformance in Multi-Biometric Systems: A Novel and ConsistentView of Fusion Strategies Based on the Sequential ProbabilityRatio Test (SPRT)," Pattern Recognition Letters, vol. 31, no. 9,pp. 884-890, 2010.

[23] S. Evans and J. Wallner, "Risk-Based Security Engineeringthrough the Eyes of the Adversary," Proc. the IEEE Workshop InformationAssurance, 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 Eventsin Critical Infrastructures," Proc. Int'l Symp. High-Assurance SystemsEng. (HASE), pp. 48-55, 2012.

[25] M. Cinque, D. Cotroneo, R. Natella, and A. Pecchia, "Assessingand Improving the Effectiveness of Logs for the Analysis of Softwarefaults," 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. IEEEInt'l Symp. Dependable Computing (PRDC), pp. 313-322, 2008.

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

About Authors:

K.Sravanthi is currently pursuing her MCA in MCA Department, QIS College of Engineering and Technology, Ongole, A.P.