Web & Android Authentication Model using User Verification Techniques

Suvarna D. Pingle

[1] *Associate Professor , PES College of Engineering,Aurangabad*

ABSTRACT

Abstract— This Security of web services is a concern in the present. Secure user authentication is essential and fundamental in most systems. Authentication and authentication systems typically use a pair of usernames and passwords, and only authenticate the user during the login session. No sessions were checked during a session that was canceled by a clear lock or expired after the user's idle session. An emerging biometric solution replaces the user name and password of a user with biometric attributes and data during creation and session access. In this way, one-time verification is not enough, and user credentials are considered permanent throughout the session. The solution is to use a short session timeout period and ask users to enter their credentials periodically, but this is not a definitive solution and is a great punishment for service and satisfaction. User Satisfaction This article explores the interesting options offered by using biometric conferencing. Secure protocols for continuous monitoring are constantly monitored by users. Finally, the use of biometric data validation ensures that credentials are transparent without informing users or interacting with them in order to guarantee better service.

Keyword *Key Android Based Biometric Authentication, Web based Authentication, Trust Level, Sub trust level.*

1. Introduction

In this age of technology, web application security is a major concern due to the increasing frequency and complexity of cyber attacks, the biometric technique offering new solutions for auditing. Secure and reliable user identity by user name and password. Biochemical character of password

Biometrics is the science and technology of determining the physiological and behavioral characteristics of biometrics, including retinal scan, fingerprint recognition and fingerprint recognition, handwriting recognition, speech recognition, and keyboard BIOS. In fact, similar to a normal authentication process that relies on user names and passwords, a user's biometric data is formatted once, providing only user-specific verification. During sign-in, require at least one biometric feature. Once the credentials of the user are verified, the system will be available for the specified period or until the user logs out. This method is also sensitive to attack because user identities will remain constant over time. Suppose we consider this simple scenario: The user logs on to the critical security service, then the user leaves the PC without having to put it in the workspace while the user session is running, which allows the impersonator to deceive. In this scenario, services that the user can easily authenticate may be brought to the attention of the user.

The solution for this is to wait a bit and ask the user to re-enter the login information. But this is not a satisfactory solution. To identify inappropriate use of resources at the right time and avoid this problem, solutions are being offered that use a continuous metadata biometrics solution, which translates into user authentication. Use as a continuous process instead of a single check. Biometric data validation is based on multiple biometric features. Finally, the use of biometric authentication ensures that credentials are transparent without requiring users to re-enter data, guaranteeing system security through legacy systems.

The methods we use in WAAM for highly secure and active user sessions. The same biometric approach is offered in the biometric multiprocessor module, which adjusts and refreshes the session timeout by trust. This global credential client is evaluated as a numerical value, which is calculated by evaluating both the user and the biometric pocket data used to obtain the biometric data in each WAAM context. It includes all necessary software components. Receive and monitor biometric features, including sensors, algorithms, comparisons, and facilities for sending and managing user credentials. Live biometric live previews, while trusted in each subsystem, will be

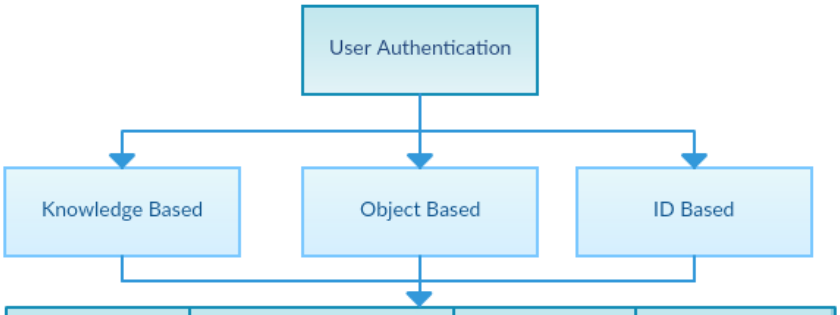
calculated. It depends on the quality and variety of sensors used for biometric sampling and the risk of being compromised.

2. Related Work:

An answer for the The key issue that continuous authentication is intended to address is the possibility that the device is used. (Smartphones, desktops, laptops, etc.) are stolen or used after a user logs in to a security or communications service. Biometric channels or biometric sensors were violated in several biometric monitoring systems designed and developed to detect the physical presence of users connected to the computer. The proposed method suggests that the user first logs in using the strict authentication procedure. Authentication process begins with several forms of biometrics. Error checking along with estimated time required to subvert the computer is automatically blocked. Similarly, in a multi-biometric authentication system, there is continuous monitoring that the user is working on the computer. If the inspection fails, the system responds by blocking the computer and delaying or terminating the user process. [8] There are several biometric serial authentication solutions. High-level access to security systems, such as ATMs, that purchase raw data in real time, is weighted in the user authentication process. I) Kind of point data ii) Availability of previous observations: Follow the availability of biometric properties. Assume that over time, the confidence in the value obtained (age) is reduced. The document uses a deterioration function that measures the uncertainty of the score calculated by the monitoring function. However, in this approach is not in continuous review, the criteria for automated multicomponent fusion will be adjusted accordingly, the principle of achieving multiple goals. The monomeric biometric system, in [3] (wrist strap), is provided for continuous user authentication and transparent login procedures in applications that users travel. When the authentication device is connected, the user can log in transparently over the wireless channel and can send authentication data to a nearby computer.

Safety assessments take years to qualitative analysis. In addition to the experimental evaluation and data analysis, [25] the quantitative safety assessment model is far from acceptable techniques, even in the area of active monitoring. The use of specific patterns for security assessments in literature has led to considerable security. An attacker tree means a faulty tree: They think that a security failure is a system failure and describes a series of events that could lead to system failure. combinatorial [14]; However, they did not think of attacking the graph. The expansion of the attack on the tree is explained by the introduction of state thought, thus providing a more complex relationship between attacks. Risk Analysis and Design Mission (MORDA) assesses the risk of a system when calculating attack scores for a set of system attacks. The ratings are based on the attacker's attack configuration and the impact of the attack. [23] Recently, the concept of social security has been adopted. [12] Support for quantitative data and support for definitions. Of the different attacker profiles.

Security systems and methods are often described as strong or weak, as shown in Figure 1. A strong system is a system with higher attack costs than the intruder's potential. Conversely, weak systems are systems where attack costs are less than potential gains. Authentication elements are grouped into three categories:
1) What do you know? 2) What you have (ie, tokens) and 3) Who are you (like biometrics)?



Referred as	Password	Token	Biometric Data
Authentication	Secrecy	Possession	Personlization
Security	Less effective with use	Insecure if lost	More secure
Digital	Computer Password	Key less entry	Face Fingerprint

Chart - Authentication Grouping

A. Knowledge-Based ("What You Know")

These data are confidential and contain passwords. Long passwords contain a single phrase and a PIN (Personal Identification Number) that is maintained for verification purposes. However, there are loopholes in the authentication model that use passwords. The basic disadvantage of passwords is that unforgettable passwords are often guessed or searched by intruders, and randomly changing passwords is difficult to remember. In addition, every time authentication is shared, it is not confidential. They did not provide a good compromise review and they did not provide critical defense to the refusal.

B. Object-Based ("What You Have")

They have a physical appearance, possession, or token. Security Token [13] Access Token or Token is a physical device that is authenticated. This may be a secure storage device that has passwords, such as a bank card, token card, smart card, and so on. One is to store or create multiple code passwords. The second advantage is to check the compromise. The third advantage is the decline in service. Two major disadvantages of tokens are inconvenience and expense. There are also opportunities to be lost or stolen. However, there are different advantages to using physical objects used to authenticate. If lost, the owner sees this evidence and can follow it.

C. ID-Based ("Who You Are")

They are unique for one person. Driver's license, passport, etc. are all in this category. Biometric data such as facial fingerprints, voiceprint scans or signatures. One advantage of biometrics is that they can not be stolen more easily than other monitors, so they have better protection against rejection of ID documents and biometric data. These data are difficult. However, if the biometric is compromised or the document is lost, the password can not be easily changed, such as a password or a token.

3. System Architecture

The architecture is divided into two phases, user can access web service and also Android phone service for secure authenticated access.

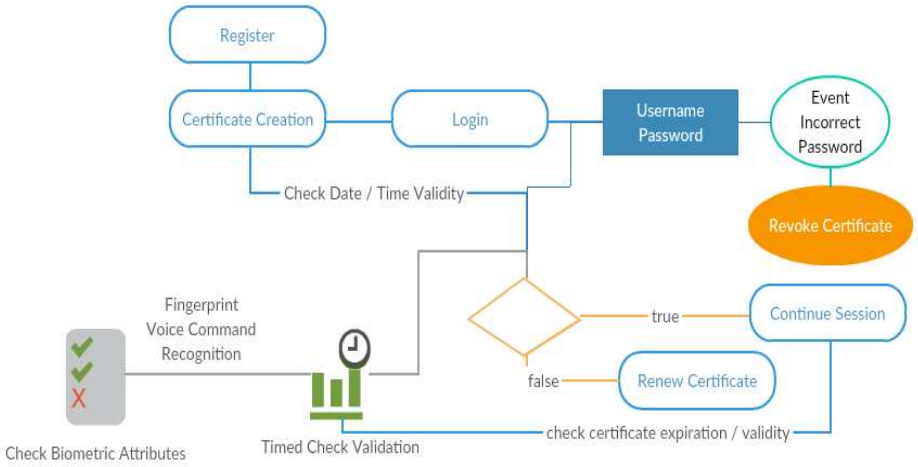


Chart -2 Web access service

3.1 Web Access Service Model

The system architecture consists of Web Access and Authentication Model (WAAM) clients and web services, and is connected via a communication channel. Figure 2 describes the continuous authentication system for Web services. An authentication server that interacts with a client server. Calculation using a biometric data comparison for user authentication and template database includes user biometric data (required for user authentication or verification.). Web services [15] [16] require user authentication to the WAAM authentication server. These services are an Internet service. Any type In the end, in the customer segment, we refer to the user's device. (Laptops, PCs, tablets, etc.) that receive biometric data that correspond to the different biometric characteristics of the user and transmit data to the WAAM-based authentication server. Specific web.

The client contains: i) Certificate: to receive raw data ii) The WAAM application sends raw data to the authentication server. The WAAM Authentication Server uses authentication and user authentication processes that compare raw data with stored digital certificates. Consider the online service that users want to access online services using a smartphone. Web users and services must be enrolled in WAAM authentication services and users must have the WAAM application installed on their smartphone. Smartphones contact the online banking service [5] which responds by asking the customer to contact the WAAM authentication server and obtain the authentication certificate. Using the WAAM application, the smartphone sends unique biometric identifiers and information to the authentication server for authentication.

The authentication server authenticates a user's credentials and gives access if: i) is registered in the WAAM authentication form; ii) has access to the online service; and iii) The biometric data obtained corresponds to the data stored therein. The database template associated with the supplied identifier. In the case of successful user authentication, the WAAM authentication server issues client authentication certificates, which authenticate to third parties, and include the maximum waiting period for the session. Of users The client presents this certificate to the web service, which monitors and gives access to the WAAM client application to keep the session open continuously: It receives transparent biometric user information and sends it to the client. WAAM authentication server to obtain a new certificate. Such certificates, including new waiting times, will be forwarded to the web service to increase the user duration.

3.2 Process

The user authentication process is based on user name, password, and binary biometric user authentication. Once the credentials of the user are verified, the system will be available for the specified time period or until the user explicitly closes the session.

Active user sessions allow intruders to imitate users and access personal information that may be misused. [1]

The system provides a new way to continuously monitor users, which continually collects biometric data.

Turn user verification to on-going process rather than single event.

This system provides an effective authentication system for secure Internet services, which provides continuous and transparent user authentication using biometric features.

CA (Continuous Authentication) system architecture [16] [17] [18] protects web services. The system also detects misuse of the device and avoids malicious activity based on biometric multi-format continuous authentication.
Biometric Techniques [17] [18] Offers a solution for accurate and reliable verification. User sessions are open and secure, even though there is a potential user inactivity activity, while there is a potential misuse detection by continuously validating the user.
related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work.

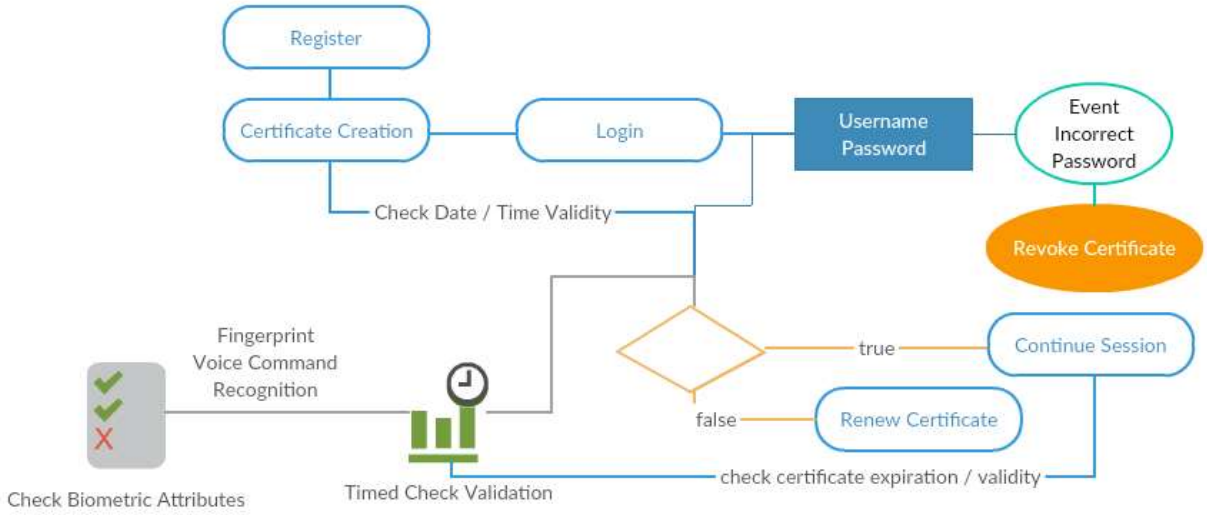


Chart -3 Android Authentication Model

3.3 Two consecutive phases:

1. The initial step is intended to monitor users on the system and establish a session with the web service.
2. During session maintenance, updates will be updated when a user identity verification process is performed using the new raw data provided by the client to the WAAM authentication server.
Initial Phase
The client first communicates with the WAAM authentication server. The first step is to receive and send the time t0 to the data for different biometric properties, which are selected for rigorous authentication procedures.
The application explicitly identifies the biometric features users must prepare and retry. The WAAM validation server analyzes the biometric data received and performs the authentication process.
This is possible in two ways. If the user's credentials are not verified. (Overall confidence level is below the municipal confidence threshold). New or additional biometric data will be requested until the lowest confidence level criterion is reached. On the other hand, if the user's ID is validated, the WAAM authentication server will verify the user calculates the initial wait time of the length T0 for the user's session. The expiration time in T0 + t0 creates. WAAM certificate and send it to the customer.
The client sends the WAAM certificate to the web service and integrates it with his request. The web service reads the certificate and allows the client to use the requested service until time t0 + T0.

3.4 Maintenance Phase

Biometric data can be purchased transparently for users. The WAAM authentication server receives the user's biometric information and authenticates the credentials of the person. If authentication is not successful, the user is marked as not an expert, and therefore the WAAM authentication server is not available.

If verification is complete, the WAAM validation server uses an algorithm to adjust the re-start time of the Ti range to the expiration of the session at Ti + ti time, and then generate and send the new certificate. With the client The user will be given a new certificate and forwarded to the web service. Ti + Ti The maintenance process consists of three steps that repeat: when the client application receives the latest raw data (new) (Matches biometric features) will communicate with the WAAM authentication server.

Biometric data can be obtained transparently for the user. However, users can decide to provide biometric data that is not likely to be purchased in a clear way. Eventually, when the session timeout expires, the client informs the user that new biometric information is required. The WAAM authentication server receives the user biometric information and authenticates the client credentials. If the check fails, the client will be marked as invalid and as a result, the WAAM validation server can not be used to improve the session timeout. Does not specify whether a user is disconnected from the current session. If another biometrics is provided before the timeout expires, you can request a new certificate and update the waiting time. If verification is complete, the WAAM validation server uses an algorithm to adjust the elasticity value at the given time. Ti is the time expiry of the session at Ti + ti time and then creates and sends a new certificate to the client. Certified clients and providers to online service providers; The web operator reads the certificate.

Performance Analysis

During the initial phase, the user trust level is simply set to g(t0). During the maintenance phase, the user trust level is computed for each received fresh biometric data. The user trust level at time ti is given by:

$$g(ti) = \frac{(-arctan((\Delta ti - s).k) + \frac{\prod}{2}).trust(t_{i-1} - 1)}{-arctan(-s.k) + \frac{\prod}{2}} \quad \text{.....(1)}$$

Value $Delta(ti) = ti - ti - 1$ is the time interval between two data transmissions; trust(ti-1) instead is the global trust level computed in the previous iteration of the algorithm. Parameters k and s are introduced to tune the decreasing function: k impacts on the inclination towards the falling inflection point, while s translates the inflection point horizontally, i.e., allows anticipating or delaying the decay.

Computation of the Session Timeout

We assume that ti + 1 is the time that the global level of trust reaches the community minimum limit, such as a (ti + 1) = Gm. The timeout is given by Ti = ti + 1 - ti to obtain the closed formula for the value we created for the first time (1) for i + 1.

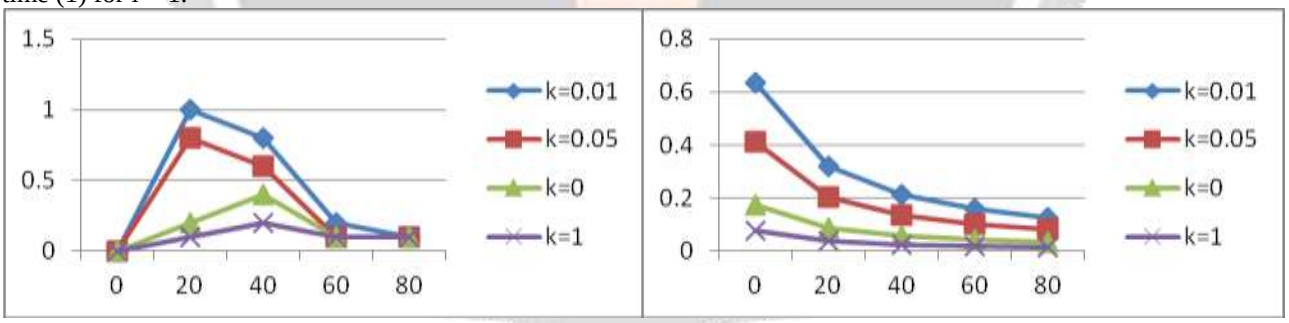


Chart -4 Computation of existing method and proposed method

Trust Levels And Timeout Computation

With the biometric unimodal Sk system, with k = 1, 2, ..., n, which can be decided depending on the accuracy of the user. FNMRk is the proportion of genuine comparison, which results in Inconsistent mismatch is a decision not a coincidence. When comparing biometric samples with the form of the same biometric source, it is possible that the Unimodal Sk system will give the user the correct breakdown.

Conversely, false rate FMRk is the possibility that the unimodal system subsystem causes a false matching error. However, the error will determine whether the invalid user is an invalid user instead of the valid word. Incorrect mismatch in unimodal system will lead to invalid user authentication.

1) Confidence and Waiting Time Algorithm An algorithm for displaying duplicate session expiration times on the WAAM authentication server. Requires new waiting times and expiration times. WAAM server validation receives new biometric data from users. Consider that the initial phase occurs in time □0 upon receiving biometric data and

passing the application. (We assume that this information is sent to the WAAM authentication server and leads to satisfactory confirmation.) The algorithms described below are run to assist in reading. U is often overlooked. For example, g (ti) = g (u, ti)
2) Calculation of confidence in the subsystem. Algorithm starts to calculate the confidence in the subsystem. Intuitively, the confidence level of the subsystem can be created in a constant m (Sk, t) = 1 - FMR (Sk) for each Unimodal Sk subsystem, and at any time t (we assume that the data in the system Its use includes the FMR. It has Edam repository accessible by the WAAM authentication server.) But we use the punishment function to measure the trust in subsystems based on usage. In general, in our approach, the less subsystem you use, the more reliable you are to prevent malicious users from using only biometric features. (For example, through imitation sensors) to be able to authenticate online services. Rely on reusable subsystems to obtain biometric data.
3) User Confidentiality Due to the recent user identity verification time, this user is likely to be replaced by a legitimate user who is: Decline in user confidence This allows us to simulate the level of user confidence over time using reduced functionality. i) reduce asymptotically to zero ii) give confidence (, □□ - 1) for Δti = 0 and iii) can be adjusted with a parameter The two controllable delays and slopes (k), where the confidence level decreases with time.

The information contained in the content of the WAAM certificate sent to the user through the WAAM authentication server is essential to realizing the key points of this process. The WAAM certificate consists of a timestamp and a unique sequence number identifying each certificate, and is responsible for replicating the attack. Id is an identifier such as a number. The option represents the end result of a server-side validation process. Total session timeout defined by dynamic WAAM authentication server. Typically, the global confidence interval and the waiting period of a session are always calculated considering the interval as soon as the WAAM application receives biometric data to limit the probability of unknown delay. In the discussion and calculation. Since such delays are unpredictable in the past, just providing a relative timeout value for a user is not possible. Therefore, the WAAM server will provide the time when the session should expire.
WAAM certificate expires when expiry time reaches zero.

4. CONCLUSIONS

The session management system uses the user name and password completely, and the session is canceled by explicitly logging out or by expiration of the session timeout. Continuous identification method using different biometrics. First Sign-In Corruption is not sufficient for the risk associated with a signed post in a session. We take advantage of new possibilities offered by biometrics to define protocols for continuous authentication to improve the security and usability of user sessions. The protocol calculates an adjustable timeout period based on trust in user activity and the quality and type of biometric data acquired transparently by background checks of user actions. Continuous authentication using multiple biometrics enhances the security and usability of the user. The proposed function for evaluating session timeouts is selected between a set of possible alternatives.
In this project, the WAAM protocol is used for continuous authentication, which enhances the security and usability of the user session. The protocol calculates adjustable timeouts based on trust in user activity and on the quality and type of biometric data acquired transparently by background checks of user actions. This authentication system provides a new way of authenticating user credentials in real time through the use of biometrics features. This system represents a powerful biometric use to identify users. correct It also validates the physical identity of the user through continuous biometric data. Authentication can always achieve a balance between security and usability by constantly monitoring the user and being transparent. Consistent authentication with Biometrics enhances the security and usability of user sessions.

5. REFERENCES

[1]. [1] CASHMA -Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
[2] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli ”Continuous and Transparent User Identity Verification for Secure Internet Services” IEEE Transaction on De-pendable and Secure Computing, VOL. 12,NO. 3,JUNE 2015
[3] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, ”Biometrics: A Grand Challenge” International Conference on Pattern Recognition , Aug 2004.

[4] 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.
[5] T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,," Banking & Technology Snapshot, DB Research, Feb. 2012.
[6] 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.
[7] 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.
[8] 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.
[9] Biometric System Base Secure Authentication Service for Session Management Nilima Deore, Prof. C.R.Barde International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015.
[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.