An economical and secured approach for continuous and transparent user identification for secure web services

P.Kalyan chakravathy[1], K.Vasavi Devi[2], T.Sai Sri[3], Sk.Abu Saleha[4]

[1,2,3,4] *Department of computer science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India –522502.*

ABSTRACT- *Nowadays, it becomes serious concern to provide more security to web services. So, secure user authentication is the fundamental task in security systems. Traditionally, most of the systems are based on pairs of username and password which verifies the identity of user only at login phase. Once the user is identified with username and password, no checks are performed further during working sessions. But emerging biometric solutions substitutes the username and password with biometric data of user .In such approach still single shot check is less effective on the grounds that the personality of client is perpetual amid entire session. Hence, a basic solution is to use very short period of timeouts for each session and periodically request the user to input his credentials over and over. But this is not a proper solution because it heavily affects the service usability and ultimately the satisfaction of users. This paper investigates the framework for ceaseless confirmation of client utilizing his qualifications, for example, biometric characteristics. The utilization of consistent biometric verification framework obtains accreditations without expressly informing the client or requiring client cooperation that is, straightforwardly which is important to ensure better execution and administration ease of use.*

KEYWORDS-Web Security, Authentication, Continuous user verification, biometric authentication.

I. INTRODUCTION:

In almost every aspect of human life have computing devices (such as PC, smart phone, tablet, or smart watches) become important gadgets. The communication services, aviation and financial services are very much controlled by computer systems. People entrust with vital information such as medical and criminal records, manage transactions, pay bills and private documents. However, this increasing dependency on computer systems, coupled with a growing emphasis on global accessibility in cyberspace, has unveiled new threats to computer system security. Moreover, violations and frauds in the internet are all over the place. For most existing PC frameworks, once the client's character is checked at login, the system resources are available to that user until he/she exits the system or locks the session. In fact, the system resources are available to any user during that period. This may be appropriate for low security environments, but can lead to session hijacking, in which an attacker targets an open session, e.g. when people leave the computer unattended for shorter or longer periods when it is unlocked, for example to get a cup of coffee, to go and talk to a colleague, or simply because they do not have the habit of locking a computer because of the inconvenience. In high risk environments or where the cost of unauthorized use of a computer is high, a continuous check of the user's identity is extremely important. By utilizing nonstop check the personality of the human working the PC is persistently confirmed. Username and secret word of conventional confirmation framework is get supplant by biometric characteristic if there should be an occurrence of biometric method. Biometrics are the science and technology of determining and identifying the correct user identity based on physiological and behavioural traits which includes face recognition, retinal scans, fingerprint voice recognition and keystroke dynamics. Username and secret word of conventional confirmation framework is get supplant by biometric characteristic if there should be an occurrence of biometric method. Only at the login time. If the identity of user is verified once, then resources of the system are available to user for fixed period of time and the identity of user is permanent for whole session. A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials again and again. To opportune identify abuses of PC assets and keep that an unapproved client malignantly replaces an approved one, arrangements in light of multi-modular bio-metric continuous authentication are proposed, turning client confirmation into a nonstop procedure rather than onetime event. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits .new approach for users verification and session management are discussed in this paper is characterized and actualized with regards to the multi-modular biometric verification framework CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture). The CASHMA framework understands a safe biometric confirmation benefit on the Internet, in this clients need to recall just a single username and utilize their biometric information as opposed to passwords to verify in various web administrations. CASHMA work safely with any sort of web benefit for instance web based managing an account, military zones, and air terminal zone which require high security administrations.

II. LITERATURE SURVEY:

The introduction to security issues & its concern is described in previous section. In this literature we have studied earlier research papers related to conventional authentication systems it presents single time authentications of the user. The categorizations of security systems are depend on

strength of attack and are classified into strong and weak. The summarizing study of earlier research is as follows:

1. Primary approach is knowledge based identity for authentication of user involves is password thai is what you know; Password contains single word, PIN (Personal Identification Number), Phrases that can be reserved secret for authentication. But this primary approach Knowledge based identity does not offer good solution it can be searched or guess by an attacker and they do not present security against repudiation [6].

2. Secondary approach is object based identity for authentication of user involves what you have is token; Token means a physical device which provides authentication that can be security tokens, access token, storage devices including passwords such as smart card or bank cards [6]. The main disadvantage of Identity token can be lost or stolen and inconvenience and cost.

3. Last approach is ID based authentication for authentication of user it considers who you are. That is simply biometric such as voice recognition, figure print identification, face recognition and signature or eye scan give stronger defence against attack. Comparing with Knowledge based and object/entity based ID based authentication provides privileged level of security.

III. THE CASHMA ARCHITECTURE CASHMA:

It means Context-Aware Security by Hierarchical Multilevel Architectures. This system is used for secure biometric authentication on the internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services. Contingent upon Preferences and prerequisites of the proprietor of the web benefit the CASHMA confirmation benefit supplant the customary verification benefit.

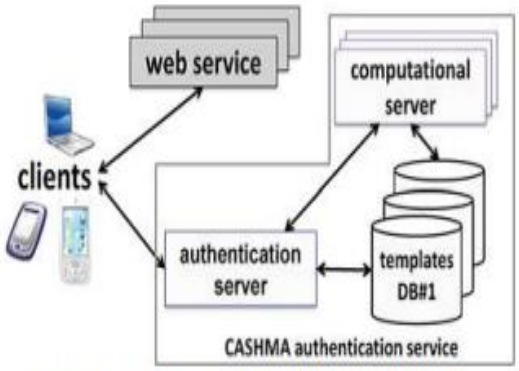

Fig.1. overall view of the CASHMA architecture

The system architecture is consisting of the CASHMA authentication service, the clients and the web services and they are connected through communication channels. Fig. 1 depicts the constant validation framework to a web benefit. The authentication server, which interacts with the clients, computational servers that perform comparisons of biometric data for verification of the users, and databases of templates contains the biometric templates of the users (that are required for user authentication or verification purpose). 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 information to the CASHMA confirmation server towards an objective web benefit.

A client contains. i) Sensors - acquire the raw data, ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA confirmation server applies client validation and check methodology that contrast the crude information and the biometric formats put away. Consider online banking where a user wants to log into an online banking service using a smart phone. Here client and web administrations must be enlisted to CASHMA validation administration and client must be introduced CASHMA application on his advanced cell. The smartphone contacts the online banking service, which replies requesting the client to contact the CASHMA authentication server and get an authentication certificate. Utilizing the CASHMA application, the cell phone sends its one of a kind identifier and biometric information to the validation server for confirmation. 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 associated 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 certificate 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 biometric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.

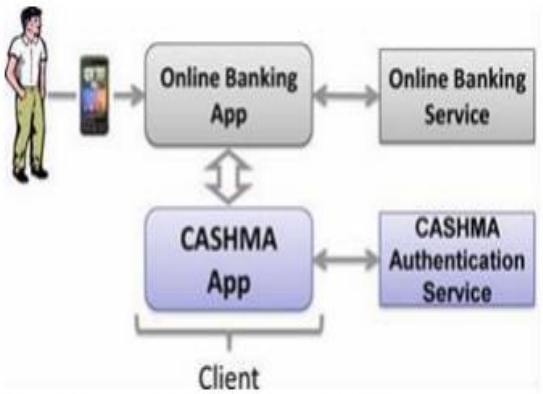

Fig2. Online Banking services using CASHMA

IV. THE CASHMA CERTIFICATE:

The data contained in the body of the CASHMA declaration transmitted to the client by utilizing the CASHMA verification server, basic to perceive imperative purposes of the convention. The CASHMA certificates consist of Time stamp and sequence number univocally identify each certificate, and it look after from replay attacks. Id is the person id, e.g., a number. Choice represents the final result of the verification process carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. Typically ,the global trust stage and the session timeout are at all times computed by way of considering the time immediate in which the CASHMA application acquires the biometric data, to restrict potential issues concerning unknown delays in conversation and computation. Due to the fact such delays will not be predicable in prior, simply supplying a relative timeout value to the user will not be viable, so the CASHMA server thus provides the absolute immediate of time at which the session must expire. The CASHMA certificates will probably be expired when the expiration timeout attain zero.

V. THE CONTINUOUS AUTHENTICATION PROTOCOL:

The continuous authentication protocol allows providing adaptive session timeouts to a web service to set up and maintain a secure session with a client. The information contained in the body of the CASHMA statement transmitted to the customer by using the CASHMA confirmation server, fundamental to see basic reasons for the tradition. The execution of the protocol is composed of two consecutive phases: the initial phase and the maintenance phase. The initial phase aims to authenticate the user into the system and establish the session with the web service. During the maintenance phase, the session timeout is adaptively updated when user identity verification is performed using fresh raw data provided by the client to the CASHMA authentication server. The user (the client) contacts the web service for a service request; the web service replies that a valid certificate from the CASHMA authentication service is required for authentication.

VI. CONCLUSIONS:

Session administration framework is completely in view of username and watchword, and sessions are ended by unequivocal logouts or by the termination of session timeouts. Techniques utilized for persistent confirmation utilizing diverse biometrics. Introductory one time login confirmation is deficient to address the hazard engaged with post signed in session. We misused the novel probability acquainted by biometrics with characterize a convention for consistent verification that enhances security and ease of use of client session. The convention figures versatile timeouts on the premise of the put stock in postured in the client movement and in the quality and sort of biometric information gained straightforwardly through observing in foundation the client's activities. Constant confirmation check with multi - modular biometrics enhances security and ease of use of client session. The capacities proposed for the assessment of the session timeout are chosen among a huge arrangement of conceivable options.

REFERENCES:

[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.