IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

Preventing the Anonymous Authentication Using Cashma Technique

Santhosh
Bharathidasan University
or.santhosh@ymail.com

Prof. Dr. V. JayaRaj
Bahrathidasan University
jaya_v2000@yahoo.com

Abstract: Security in web-based session management is a serious concern, due to the recent increase in the frequency and complexity of cyber attacks. Traditionally most of the system are based on the pairs of username and password which verify the identification of the user only at the login phase. Once the user can be identified, no checks are performed during the working sessions, which are terminated by explicit logouts or expire after an idle activity period of the user. In this approach, a single shot of verification is less efficient and the user identity is permanent during the entire session.

To overcome this aspect, a secure protocol authentication is used for continuous user verification. This protocol makes adaptive timeouts and periodically request the user to input his authentication attributes over and over. For this adaptive method, CASHAMA authentication system is used which provides different verification methods such as Keystroke timing, Mathematical event, and CASHMA certificate. The use of this CASHMA system will provide secure web service and prevent the loss of data.

Keywords: Web Security, Authentication, Continuous User Verification

I.INTRODUCTION

The usage of web based applications and technologies are increased rapidly day by day. There are many events that have been directed our attention towards the usage of a web-based application with safety and security. Therefore security of such web based applications is important and necessary part of today's technology. Security can be provided on the basis of Authentication, Authorization and Session management.

1.1 Session Management:

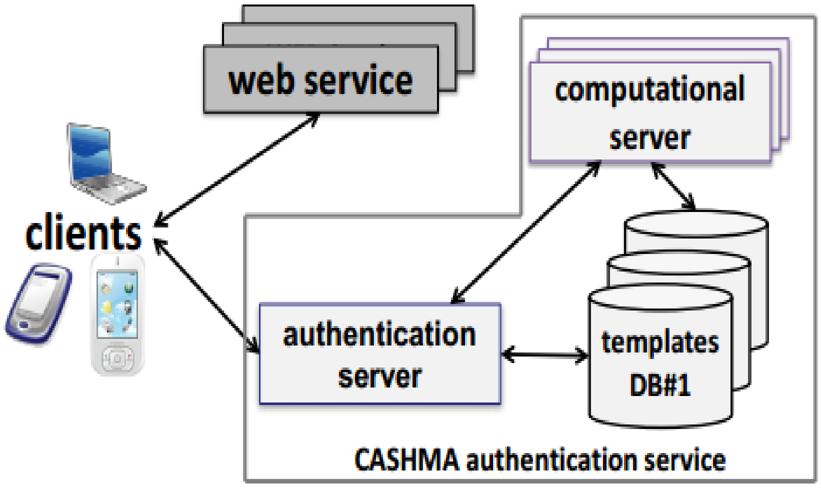
The term user Session refers to a series of user application interactions that are tracked by the server. Sessions are used for maintaining user-specific state, including persistent objects (like handles components or database result sets) and authenticated user identities, among many interactions. For example, a session could be used to track a validated user login followed by a series of directed activities for a particular user. Session management in distributed internet services is traditionally based on Username and Password. These authentication methods for the required session will identify the user only at the login phase.

1.2 CASHMA Authentication:

A new approach for user verification and session management that is applied in the CASHMA (Context Aware Security by Hierarchical Multilevel Architectures). The overall system is composed of the CASHMA authentication service, the clients and the web services (Fig.1) connected through communication channels. Each communication channel in 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 comparisons 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 CASHMA application operates to continuously maintain the session open: it transparently acquires data from the user and sends them to the CASHMA authentication server.

Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.



The CASHMA Certificate:

The CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol. *Timestamp* and *Sequence number* univocally identify each certificate and protect from replay attacks.

1.3 The Continuous Authentication Protocol:

The Continuous authentication protocol allows providing adaptive session timeouts to a web service for setting up and maintain a secure session with a client. The timeout is adapted on the basis of the trust that the CASHMA authentication system puts in the secure subsystems and in the user. A promising form of continuous authentication is centered on unique human behaviours. Known as behavioural biometrics, these tools can monitor things like keystroke patterns which analyze typing rhythm, mouse movement, iris patterns and more.

The execution of the protocol is composed of two consecutive phases:
i) *The initial phase* and ii) *the maintenance phase*.

The *Initial phase* (Fig.2) aims to *authenticate* the user into the system and establish the session with the web service.During the *maintenance phase*,(Fig.3) the session timeout is adaptively updated when *user identity verification* is performed.

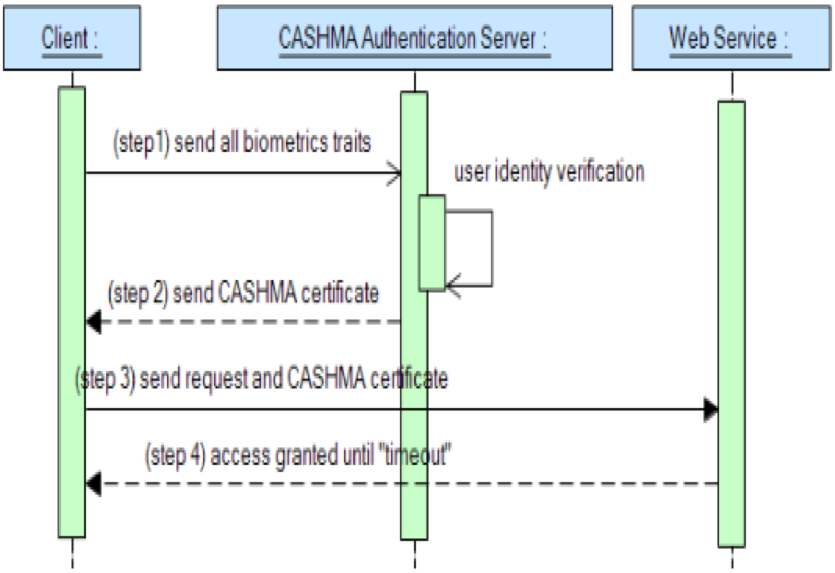

Client :
CASHMA Authentication Server :
Web Service :
(step1) send all biometrics traits
user identity verification
(step 2) send CASHMA certificate
(step 3) send request and CASHMA certificate
(step 4) access granted until "timeout"

Fig.2 Initial Phase

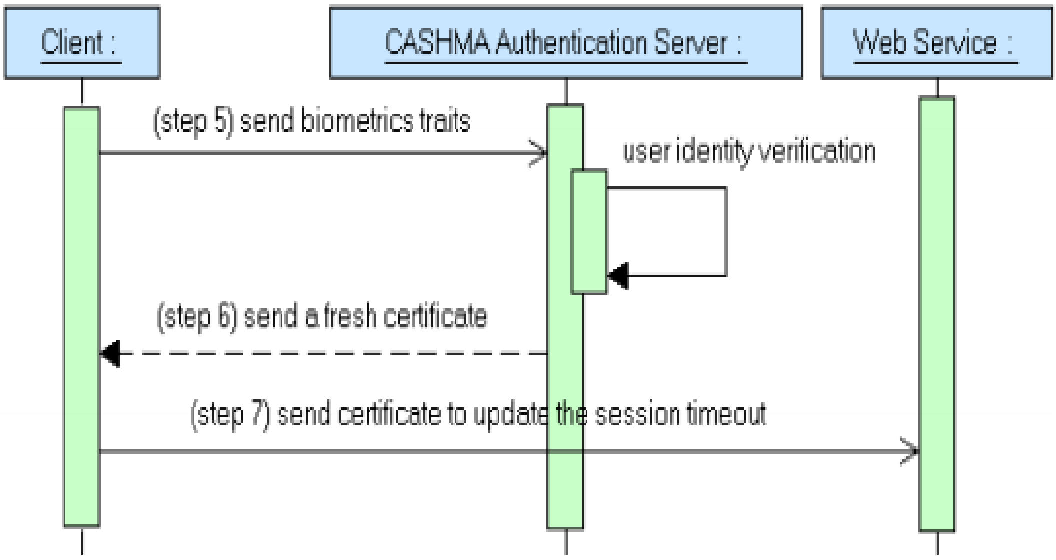

Client :
CASHMA Authentication Server :
Web Service :
(step 5) send biometrics traits
user identity verification
(step 6) send a fresh certificate
(step 7) send certificate to update the session timeout

Fig.3 Maintenance Phase

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.

II.LITERATURE SURVEY

2.1: Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. 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.

2.2: Security of the web-based services becomes serious concern nowadays. Secure user authentication is very important and fundamental in most of the systems User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users

2.3: In the field of internet services secure internet services is an important issue. Traditional distributed internet services are based on session management of username password, logouts and user session expiration timeouts. Biometric authentication provides a solution to substitute password with biometric information in session creation with single verification. In proposed work, an additional level of security can be provided & multiple verifications can deploy for authentication.

2.4: The universal adoption of the Internet and the emerging web services technologies constitutes the infrastructure that enables the provision of a new generation of e-services and applications. However, the provision of e-services through the Internet imposes increased risks, since it exposes data and sensitive information outside the client premises. Thus, an advanced security mechanism has to be incorporated, in order to protect this information.

III.MODULES

- ➢ Keystroke Dynamics
- ➢ CASHMA Authentication
- ➢ Misspelt Word
- ➢ Keystroke Timing

MODULES DESCRIPTION

- ✓ **Keystroke Dynamics**

The keystroke rhythms of a user are measured to develop a unique biometric template of the user's typing pattern for future authentication. It measurements available from almost every keyboard can be stored even recorded to Dwell timing of key pressed and the time between "key up" and the right next "key down". The saved keystroke timing data is then processed through a unique and specific neural algorithm, which determines a primary pattern for future comparison.

- ✓ **CASHMA Authentication**

Password collection by keystroke and related malware is increasing at an alarming rate. The attacker can make them stop working heuristics to impute missing latency values or only selected latencies from a victim, to generate desired text or system commands. It provides a trusted path to the user for obtaining authentication credentials. Although generally stateless, it can store temporary session keys and may optionally act as a password manager. This page could be completely under the control of spyware, or it could be controlled by an online site in-the-middle.

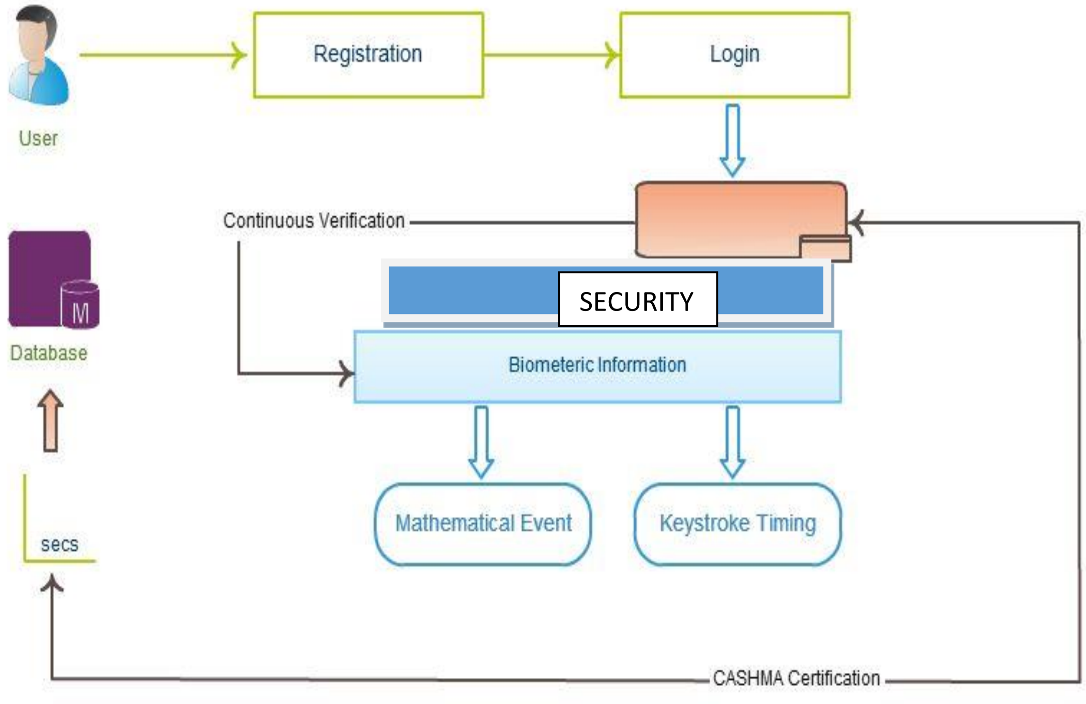
- ✓ **Misspelt Word**

Calculate the rate of Misspelt word when the user types the text wrongly. This performs the step when the number of times each of the words whose misspellings are being identified was found in the entire text body is counted and recorded. The attacking can be found then this recorded rate match with the original latency of the text. The attack can be found and mitigated when the calculated score does not match the original record of data.

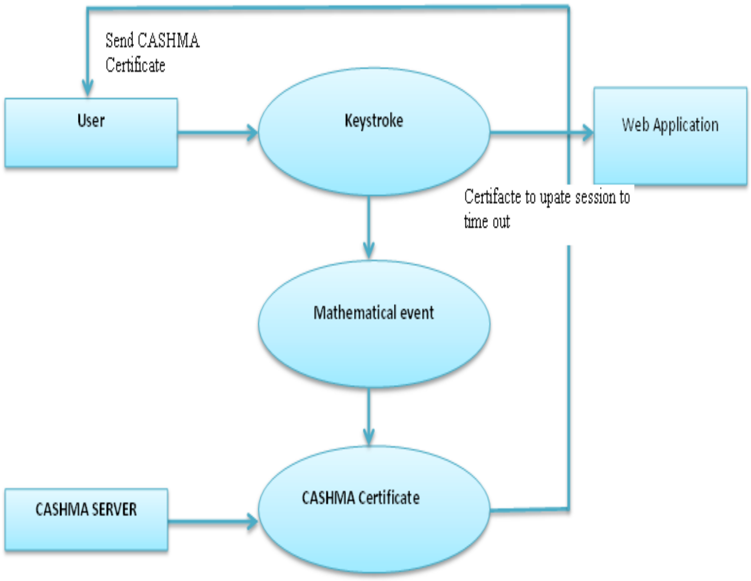
- ✓ **Keystroke Timing**

We present the keystroke timing information, if the typed the text this is text, the attacker records a series of time stamps (the time when was pressed), (the time when was released), and so on. The participants were allowed to make spelling mistakes, typographical errors and if they chose, could correct them using Backspace or Delete keys. The keystroke data collection software provided for typing copy and self-texts. The results additionally show that effective keystroke forgeries can be created with a) as low as 20 to 100 characters of text and keystroke timing information.

IV.SYSTEM ARCHITECTURE



>> Block Diagram



- The block diagram shows the process of CASHMA authentication process, with the user attributes such as

✓ Keystroke Dynamics
✓ Mathematical event
✓ CASHMA certificate.

V. SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

>> Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at the component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

>> **Integration testing**

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

>> **Functional test**

Functional tests provide systematic demonstrations that function tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:
Valid Input: identified classes of valid input must be accepted.
Invalid Input: identified classes of invalid input must be rejected.
Functions: identified functions must be exercised.
Output: identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests are focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages, and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

CONCLUSION

Session management is a serious concern in the web services. Once the user can be identified, no checks are performed during the working sessions, which are terminated by explicit logouts or expire after an idle activity period of the user. In this approach, a single shot of verification is less efficient and the user identity is permanent during the entire session.

For this security drawback, a secure protocol authentication is used for continuous user verification. This protocol makes adaptive timeouts and periodically request the user to input his authentication attributes over and over. For this adaptive method, I am using CASHAMA authentication system which provides different verification methods such as Keystroke timing, Mathematical event, and CASHMA certificate. The use of this CASHMA system will provide secure web service and prevent the loss of data.

ACKNOWLEDGEMENT

First and foremost I would like to thank **MY FAMILY** for the abundant shower of grace blessings on me throughout my entire project. I wish to express my deep sense of gratitude to **Dr. Gopinath Ganapathy Ph.D., Head, School of Computer Science, Engineering and Applications, Bharathidasan University, and Tiruchirapalli-23** for giving me this opportunity to do this project work. I would like to express my genuine regard and respect to my project guide, **Dr.V.Jayaraj**Associate Professor**,** Department of Computer Science & Engineering**,** School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirapalli-23for her encouragement and guidance in carrying out this project work successfully. I wish to thank our coordinator **Dr. Smitha Evelin Zoraida, M.Sc., M.Phil., Ph.D., Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli-23** for being a moral support to me and for his endless support. Lastly, I wish to express heartfelt thanks to all the faculty members of Computer Science department and friends who helped me either directly or indirectly to complete this project.

REFERENCE

1. "Continuous and Transparent User Identity Verification For Secure Internet Services" Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Margugli
2. https://www.google.com
3."Multiple Verification for Continuous Secure User Authentication"Poonam Mahale, Mr. Niranjan Bhale
4." A Dynamic Context-Aware access control architecture for e-services" Vassilis Kapsalis, Loukas Hadelli, Dimitris Kareli, Stavros Koubias
5."A Survey on Continuous User Identity Verification Using Biometric Traits For Secure Internet Services"Harshal A. Kute, D. N. Rewadkar
6. Keystroke dynamics as a biometric for authentication
Fabian Monrose a,∗, Aviel D. Rubin