Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

User Identification for Secure Net Services

Sindhuja Rangishetty
Department of computer Science Engineering,
TKR College of Engineering and Technology,
Medbowli, Meerpet, Saroornagar, Hyderabad-500097, India.

K.V.Prasad
Department of computer Science Engineering,
TKR College of Engineering and Technology,
Medbowli, Meerpet, Saroornagar, Hyderabad-500097, India.

A.Suresh Rao
Department of computer Science Engineering,
TKR College of Engineering and Technology,
Medbowli, Meerpet, Saroornagar, Hyderabad-500097, India.

Abstract:
Session management in distributed web services is historically supported username and password, specific logouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions enable work username and password with biometric information throughout session institution, however in such an approach still one verification is deemed decent, and therefore the identity of a user is taken into account changeless throughout the whole session. Additionally, the length of the session timeout might impact on the usability of the service and resulting consumer satisfaction. This service explores promising alternatives offered by applying biometry within the management of sessions. A secure protocol is outlined for perpetual authentication through continuous user verification. The protocol defines adjustive timeouts based on the quality, frequency and type of biometric data transparently picked up from the user. The purposeful behavior of the protocol is illustrated through Matlab simulations, whereas model-based measure is disbursed to assess the flexibility of the protocol to distinction security attacks exercised by totally different styles of attackers. Finally, this model for PCs and mechanical man smartphones is mentioned.

Introduction:
Secure user authentication is fundamental in most of modern ICT 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. Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks; biometric techniques offer emerging solution for secure and trusted authentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors. Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a “single shot”, providing user verification only during login phase when one or more biometric traits may be required [1].

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.

Cite this article as: Sindhuja Rangishetty, "User Identification for Secure Net Services", International Journal of Research in Advanced Computer Science Engineering, Volume 3 Issue 6, 2017, Page 39-47.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

For instance, we consider this simple scenario: a user has already logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while. This problem is even trickier in the context of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence .

To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits. Finally, 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 [2]. We present some examples of transparent acquisition of biometric data. Face can be acquired while the user is located in front of the camera, but not purposely for the acquisition of the biometric data; e.g., the user may be reading a textual SMS or watching a movie on the mobile phone. Voice can be acquired when the user speaks on the phone, or with other people nearby if the microphone always captures background. Keystroke data can be acquired whenever the user types on the keyboard, for example, when writing an SMS, chatting, or browsing on the Internet.

This approach differentiates from traditional authentication processes, where username/password are requested only once at login time or explicitly required at confirmation steps; such traditional authentication approaches impair usability for enhanced security, and offer no solutions against forgery or stealing of passwords. 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., smartphones, 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.

The approach we introduced in CASHMA for usable and highly secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system) multi-modal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data [1]. In the CASHMA context, each subsystem comprises all the hardware/software elements necessary to acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for data transmission and management. Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each subsystem is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

intruded. Exemplary runs carried out using Mat lab are reported, and a quantitative model-based security analysis of the protocol is performed combining the stochastic activity networks (SANs) and Adversary View Security Evaluation (ADVISE) formalisms. The driving principles behind our protocol were briefly discussed in the short paper, together with minor qualitative evaluations [9]. This paper extends both in the design and the evaluation parts, by providing an in-depth description of the protocol and presenting extensive qualitative and quantitative analysis.

EXISTING SYSTEM:

- Once the user's verified the identity the system assets are available for the period of time or until the user logout from the system. This approach assumes that one verification (as the start of the session) is spare, which the identity of the user is constant throughout the complete session.

In presented, the biometric verification system is designed and developed to detect the objective presence of the user logged in a computer. In this paper, as the result biometric continuous authentication limited access to high- protection systems as ATMs, where the rare data acquired are one-sided in the user verification process, based on i) the type of biometric qualities ii)because different sensors are able to give data with different point of timing iii) introduces the integration technique that depends on the provision of past observations: supported the idea that as time passes, the arrogance within the noninheritable (aging) values decreases . The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function [3].

DISADVANTAGES OF EXISTING SYSTEM:

• None of existing approaches supports continuous authentication.

• Rising biometric substitute username and password with biometric data during session firm, but in such an move toward still a single verification is deemed satisfactory and the identity of a user is considered absolute during the entire session.

PROPOSED SYSTEM:

• This presents a new approach for user certification and gathering organization that is applied in the context alert security by hierarchical multilevel architectures (CASHMA) system for secure biometric validation on the Internet.

• CASHMA is able to operate firmly with any kind of web check, including air force with high security demands as online bank services, and it is proposed to be used from different customer procedure, e.g., smartphones, Desktop PCs or even biometric kiosk placed at the entrance of secure areas. Relying on the choice and chock of the holder of the web service, the cashma authentication provider can suit a fixed verification provider, or can update it.

• Our regular endorsement advance is grounded on clear possession 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.

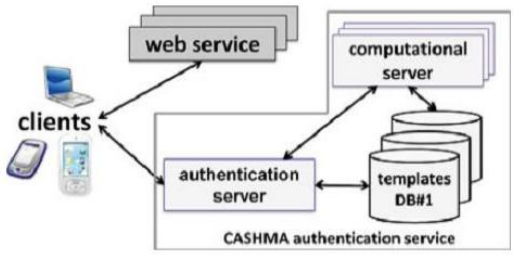
ADVANTAGES OF PROPOSED SYSTEM:

• In advance does not require the answer to a user verification variance is executed by the user device (e.g., the logout procedure), but it is clearly handled by the CASHMA certification service and the web services, which apply their own reaction.

• Provides a transaction between usability and safety.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

SYSTEM ARCHITECTURE:



LITERATURE SURVEY:

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

AUTHORS: L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,

Biometric authentication is a security process that relies on the unique biological of an individual to verify 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 plan we execute a safety estimate of the CASHMA multi-biometric confirmation system, assess the security provide by special system configurations against attacker with dissimilar capability. The adversary View Security Evaluation (ADVISE) model . An ADVISE atomic model consists of an attack execution graph (AEG) composed of attack steps, system state variables, and attack goal, as well as an adversary side view that defines the ability and benefit of a exacting adversary. 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 [6].

2. Model-view estimate of scalability and protection tradeoffs: The study on a multiservice platform

AUTHORS: L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and

Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security problems to be round-faced arise from exposing applications and knowledge to the net, so requiring an attentive analysis of potential threats and therefore the identification of stronger security mechanisms to be enforced, which can manufacture a negative impact on system performance and measurability properties. The paper present a model-based estimate of scalability and safety tradeoffs of a multi-service web-based display place, by evaluating the beginning of security mechanism may lead to a poverty of presentation property. The evaluation focuses on the 6 OPENNESS platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model and the evaluation of different configuration by composing them in different ways [5].

3. Biometric Systems: Case Study in Fingerprints

AUTHORS: U. Uludag and A.K. Jain

In spite of many return of biometrics-based creature verification systems over usual security systems based on token or information, they are vulnerable to attacks that can decrease their security considerably. In this we analyze these attacks in the area of a fingerprint biometric system.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

We propose an hit system that use a hill climb progression to create the aim guide and approximation its risk with wide check results conducted on a large fingerprint trace. Some events that can be utilize to reduce the chance of such attacks [4].

4. Automated Generation and Analysis of Attack Graphs

AUTHORS: O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing

An integral part of model the universal view of network protection is construct the aggression graph. Physical attack graph structure is boring, error-prone, and unworkable for attack graphs bigger than a hundred nodes. In this we present an automatic practice for generate and analyze attack graphs. We base our procedure on representative model checking algorithms, letting us construct attack graphs by design and professionally. We also describe two analyses to help make a decision which attacks would be most cost-effective to protector against. We implement our method in a tool suite and experienced it on a small system example, which includes models of a firewall and an interference discovery system [8].

5. Risk-Based Security Engineering through the Eyes of the Adversary

AUTHORS: S. Evans and J. Wallner

Today, security engineering for complex systems is typically done as an ad hoc process. Taking a risk-based security engineering approach replaces today's ad hoc methods with a more rigorous and disciplined approach that uses a multi-criterion decision model. This approach builds on existing techniques for integrating risk analysis with classical systems engineering. A resulting security metric can be compared with cost and performance metrics in making engineering trade-off decisions [7].

USER MODULES:

- System Model
- Authentication Server
- CASHMA
- Authentication

MODULES DESCRIPTION:

System Model:

• In this module, we create the System model to evaluate and implement our proposed system. CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it will grant access to physical secure areas as a restricted zone in associate landing field, or a military zone (in suchcases the authentication system may be supported by biometric cubicle placed at the doorway of the secure area)."User Id" refers to the identity of the user obtained from the Bank for the aim of work into the web Banking facility provided by the Bank.

• "Login Password" could be a distinctive and at random generated word well-known solely to the client, which may be modified by the user to his/her convenience. This is a method of authenticating the user ID for work into web Banking.

• “Transaction password” may be a distinctive and indiscriminately generated arcanum illustrious solely to the client, which may be modified to his/her convenience. This is a method of authentication needed to be provided by the client for golf shot through the dealing in his/her/their/its accounts with Bank through net Banking. While User ID and arcanum square measure for valid access into the net application, giving valid dealings arcanum is for authentication of transaction/requests created through net.

Authentication Server:

• In web banking like ancient banking ways, security may be a primary concern. Server can take each precaution necessary to make sure your info is

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

transmitted safely and firmly. The most recent ways in web industry security square measure won't to increase and monitor the integrity and security of the system.

• The Server maintains the functionality:

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

CASHMA:

• In this module, we present the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol. 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 world trust level and also the session timeout area unit forever computed considering the time instant within which the CASHMA application acquire the biometric information, to avoid potentials issues concerning unknown delays in communication and computation.

Authentication:

• A secure protocol is outlined for perpetual authentication through continuous user verification. The protocol determines adaptational timeouts supported the standard, frequency and sort of biometric information transparently non heritable from the user. The utilization of identification permits credentials to be nonheritable transparently, i.e., while not expressly notifying the user or requiring his/her interaction that is crucial to ensure higher service usability.

• The idea behind the implementation of the protocol is that the client continuously and transparently obtains and transmits evidence of the user identity to maintain access to a web service. The main task of the projected protocol is to make and so maintain the user session adjusting the session timeout on the premise of the arrogance that the identity of the user within the system is real.

• The execution of the protocol is composed of two consecutive phases:

- o Initial phase
- o Maintenance phase

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

• System : Pentium IV 2.4 GHz.
• Hard Disk : 40 GB.
• Floppy Drive : 1.44 Mb.
• Monitor : 15 VGA Colour.
• Mouse : Logitech.
• Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

• Operating system : Windows XP.
• Coding Language : J2EE
• Data Base : MYSQL

DATA FLOW DIAGRAM:

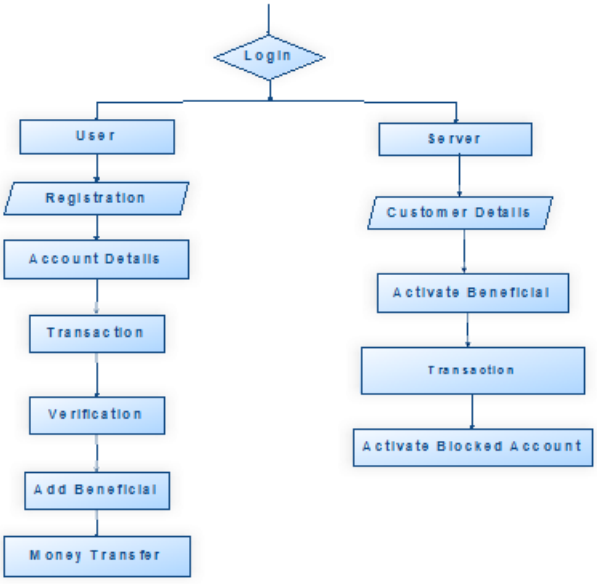
1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



UML DIAGRAMS:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML [5].

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

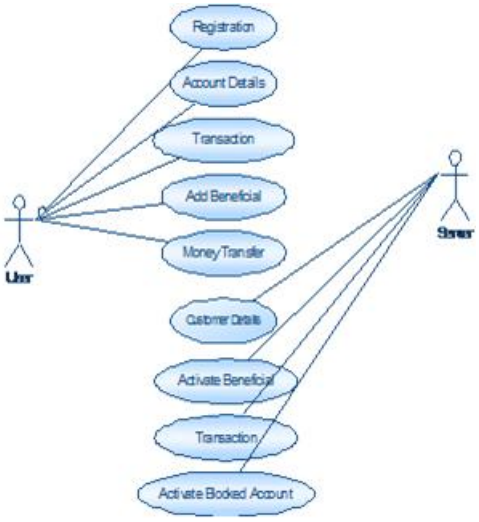
The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM:

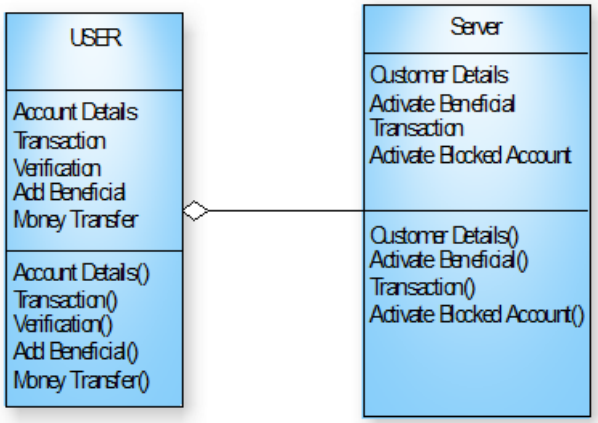
A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com



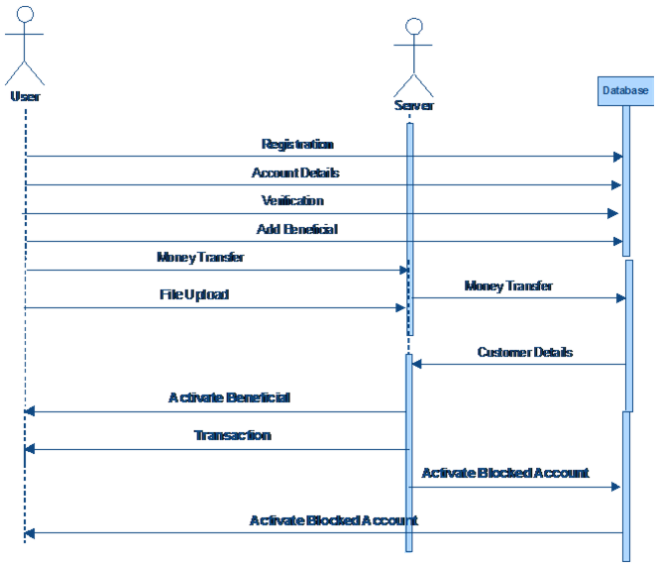
CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



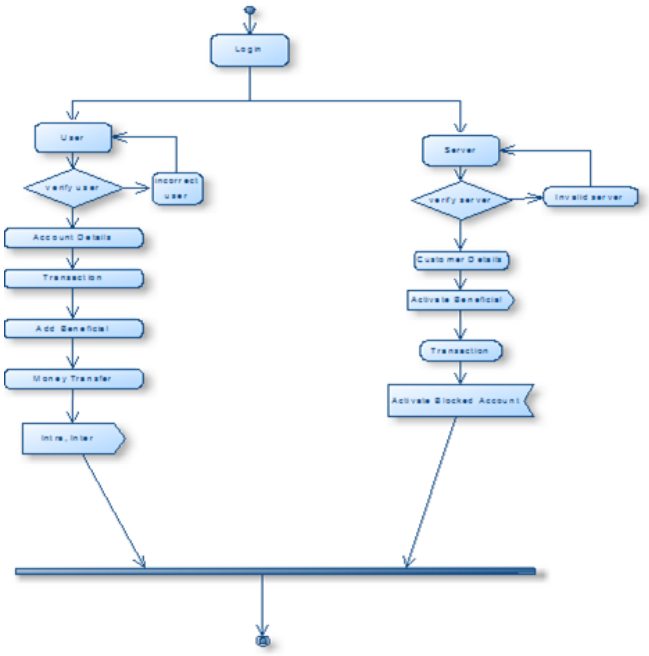
SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



CONCLUSION:

We exploited the novel risk introduced by biometry to outline a protocol for continuous authentication that

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

improves security and usefulness of user session. The protocol computes reconciling timeouts on the premise of the trust display within the user activity and within the quality and type of biometric information noninheritable transparently through observation in background the user's actions. First, the system exchanges raw data and not the features extracted from them or templates, while cripto-token approaches are not considered; as debated in Section 3.1, this is due to architectural decisions where the client is kept very simple. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be addressed considering National legislations. At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detection.

REFERENCES:

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

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

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[4] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[6] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.

[8] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

[9] C. Roberts, "Biometric Attack Vectors and Defences," Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.