International Journal of Engineering Research and Modern Education (IJERME)
ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume I, Issue I, 2016

INCESSANT AUTHENTICATION AND VERIFICATION FOR ACCESS INTERNET SERVICES

M. Steffi Ashajenet* & R. Selva Kumar**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Data gathering management in distributed Internet services is usually in light of username and password, explicit logouts and components of user session termination utilizing incredible timeouts. Increasing biometric solution permit substituting username and password with biometric information during data gathering establishment, however in such a methodology still a solitary verification is considered sufficient, and the individuality of a user is viewed as static throughout the whole session. Also, the length of the session timeout may effect on the convenience of the service and subsequent user completion. This system proposing an alternate method by applying authentication via continuous user verification by applying biometrics application in the service of sessions. A secure protocol is characterized for perpetual authentication through consistent user check. The protocol decides versatile timeouts taking into account the quality, recurrence and kind of biometric information straightforwardly procured from the client.

Index Terms: Wireless Sensor Networks (WSNs)

1. Introduction:

The System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. There exists a “communication gap” between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well- developed process. There isn’t a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

2. Related Works:

Increasing data privacy with self-destructing data was surveyed by R. Geambasu, T. Kohno, A. Levy, and H. M. Levy. The goal of creating data that self-destructs or vanishes automatically after it is no longer useful. Moreover, it should do so without any explicit action by the users or any party storing or archiving that data, in such a way that all copies of the data vanish simultaneously from all storage sites, online or offline. Numerous applications could benefit from such self-destructing data. As one example, consider the case of email. Such emails may cease to have value to the sender and receiver after a short period of time. Nevertheless, many of these emails are private, and the act of storing them in definitely at intermediate locations creates a potential privacy risk.

Defeating vanish with low-cost sybil attacks against large DHEs was surveyed by S. Wolchok, O. S. Hofmann, N. Heninger, C. J. Rossbach, B. Waters, and E. Witchel. As storage capacities increase and applications move into the cloud, controlling the lifetime of sensitive data is becoming increasingly difficult. Even if users cleanse their local files, copies may be retained long into the future by email providers, backup systems, and other services, and these may be targets of theft or subpoena. Vanish encapsulates data objects so that they “self-destruct” after a specified time, becoming permanently unreadable. It encrypts the data using a randomly generated key and then uses Shamir secret sharing to break the key into n shares where k of them is needed to reconstruct the key.

Safe vanish: An improved data self-destruction for protecting data privacy was surveyed by L. Zeng, Z. Shi, S. Xu, and D. Feng. In cloud, self-destructing data mainly aims at protecting the data privacy. All the data and its copies will become destructed or unreadable after a user-specified period, without any user intervention. Besides, anyone cannot get the decryption key after timeout, neither the sender nor the receiver. The Washington's Vanish system is a system for self-destructing data under cloud computing, and it is vulnerable to “hopping attack” and “sniffer attack”. It provide a new scheme, called Safe Vanish, to prevent hopping attacks by way of extending the length range of the key shares to increase the attack cost substantially, and do some improvement Original Vanish system.

Active storage framework for object-based storage device has surveyed by L. Qin and D. Feng. Active storage provides a service migration mechanism for applications to exploit processing capabilities in storage devices. However, in recent research, the model of service execution still remains passive request-driven mode. In self-management situation, a mechanism for automatic service execution is necessary. To address this problem, an active storage framework for object-based storage device is presented, which provides a hybrid approach to combine request-driven model and policy-driven model.

Active storage using object-based devices was surveyed by T. M. John, A. T. Ramani, and J. A. Chandy. This eliminates server as a bottleneck for data transfers between disks and clients and promises significant improved scalability through higher level interfaces. At the same time, as systems get faster and cheaper, people compute on larger and larger data sets. A large server system today will easily have a hundred disk drives attached to it. This large number of drives is necessary either to provide sufficient capacity or sufficient aggregate throughput for the target application. Taking this trend and extrapolating to future drive capabilities gives a promising picture for on drive processing. A pessimistic value for the on-drive processing already in today’s commodity SCSI disk controllers is 400 MHz, with perhaps 100 MB/s of sustained bandwidth in sequential access. This means that a system with one hundred disks has 40 GHz of aggregate processing power and 10 GB/s of aggregate bandwidth at the disks.

Typical multiprocessor systems cannot achieve these aggregate values in a single node, but computing clusters can be constructed to achieve the same capability. The advantage of the active disk cluster over a compute node cluster is the ability of the disk to manage the data directly on disk in terms of layout and scheduling. Data processing at the disk can also reduce the amount of data transferred, thereby reducing communication costs In addition, as storage is connected to a large collection of hosts by taking advantage of network-attachment and storage area networks, the interconnection network will rapidly become a principal bottleneck in large-scale applications.

An active storage system for high performance computing was surveyed by Y. Zhang and D. Feng. Traditionally, active storage devices execute custom application code on large amounts of data by utilizing the unused processing power of the storage nodes. For computation-intensive applications, the performance might be quite low due to insufficient processing power on the storage devices. In this paper we present a reconfigurable computing solution that can provide flexible, high-performance processing capabilities for the storage nodes.

3. Proposed Work:

The client application acquires fresh (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server. The biometric data can be acquired transparently to the user; the user may however decide to provide biometric data which are unlikely acquired in a transparent way (e.g., finger-print, face image). Finally when the session timeout is going to expire, the client may explicitly notify to the user that fresh biometric data are needed. The CASHMA authentication server receives the bio-metric data from the client and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not operate to refresh the session timeout. This does not imply that the user is cut-off from the current session: if other biometric data are provided before the timeout expires, it is still possible to get a new certificate and refresh the timeout. If verification is successful, the CASHMA authentication server applies the algorithm adaptively compute a new timeout of length, the expiration time of the session at time and then it creates and sends a new certificate to the client. The CASHMA Authentication server receives the bio-metric data from the client and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not operate to refresh the session timeout. Else the user is allows to access the system, and the CASHMA authentication server operate to refresh the session timeout. As time passes from the most recent user identity verification, the probability that an attacker substituted to the legitimate user increases i.e., the level of trust in the user decreases. This leads us to model the user trust level through time using a function. Different functions may be preferred under specific conditions or users requirements. It focuses on introducing the protocol, which can be realized also with other functions. The details are matched to the server and then login to the account and access the banking process. An Enrollment module, the client first registers the all information (like name, address, username, and password) to the web server. And it also register the all bio-metrics (like, fingerprint, face etc.) Authentication to the server. 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. Verify the all clients login. When the client login to the system, it verify the username, password, and all bio-metric verification within the correct session time it allows to access the system. if it’s not login the correct time does not allows access to the system. The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled user to the CASHMA authentication services. The CASHMA Authentication server receives the bio-metric data from the client and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not operate to refresh the session timeout.

Modules Description:

- ✓ Enrollment Module
- ✓ CASHMA Authentication Server
- ✓ Web service Module
- ✓ User Identity Module

Enrollment Module:

An Enrollment module, the client first registers the all information (like name, address, username, and password) to the web server. And it also register the all bio-metrics (like, fingerprint, face etc.) Authentication to the server. After complete the registration process the client can be login to the system with the correct authentication. Client we mean the users devices that acquire the biometric data corresponding to the various biometric traits from the users and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service.

CASHMA Authentication Server:

In CASHMA (Context Aware Security by Hierarchical Multilevel Architectures) certificate module, 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. Decision represents the outcome of the verification procedure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. In fact, the global trust level and the session timeout are always computed considering the time instant in which the CASHMA application acquires the biometric data, to avoid potential problems related to unknown delays in communication and computation. Since such delays are not predicable, simply delivering a relative timeout value to the client is not feasible: the CASHMA server therefore provides the absolute instant of time at which the session should expire.

Web Service Module:

In the web service module, is used to store the all information for the all clients, and it verify the all clients login. When the client login to the system, it verify the username, password, and all bio-metric verification within the correct session time it allows to access the system. if it's not login the correct time does not allows access to the system. The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled user to the CASHMA authentication services. These services are potentially any kind of internet services or application with requirement on user authenticity. They have to be registered to the CASHMA authentication services, expressing also their trust threshold.

User Identity Module:

In the user identity module, is used to identify the authorized user. The CASHMA Authentication server receives the bio-metric data from the client and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not operate to refresh the session timeout. Else the user is allows to access the system, and the CASHMA authentication server operate to refresh the session timeout.

4. Experimental Analysis and Results:

Biometrics is generally taken to mean the measurement of some physical characteristic of the human body for the purpose of identifying the person. Common types of biometrics include fingerprint, face image, and iris/retina pattern. A more inclusive notion of biometrics also includes the behavioral characteristics, such as gait, speech pattern, and keyboard typing dynamics.

When a biometric is used to verify a person, the typical process is as shown in Figure 1. The user first presents her biometric (e.g. the thumb) to the sensor device, which captures it as raw biometric data (for example a fingerprint image). This data is then preprocessed to reduce noise, enhance image contrast, etc.

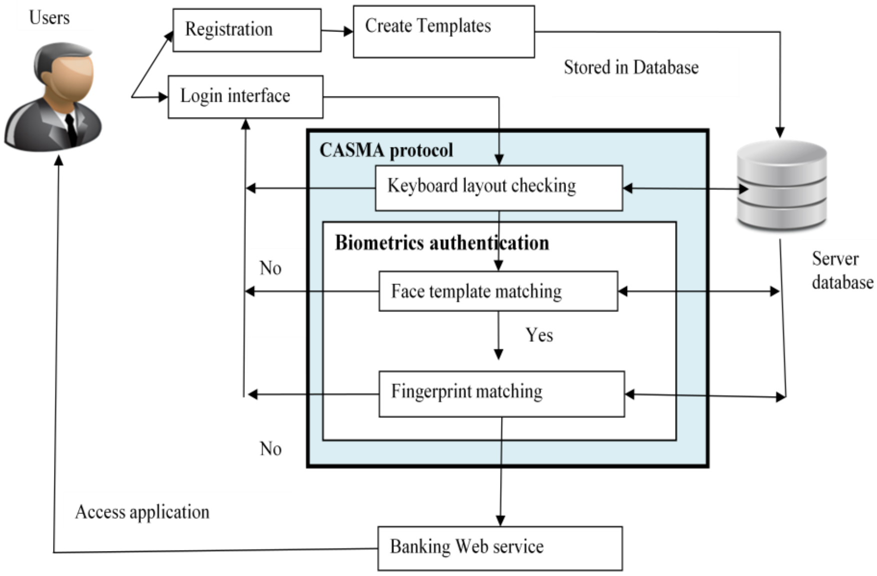

Figure 1: Architecture of Secure cloud data

Implementation of software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure that the software is meant to make their job easier. The active user must be aware of the benefits of using the system. Their confidence in the software built up. Proper guidance is impaired to the user so that he is comfortable in using the application. Before going ahead and viewing the system, the user must know that for viewing the result, the server program should be running in the server. If the server object is not running on the server, the actual processes will not take place.

5. Conclusion and Future Enhancement:

The novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. The client device uses part of its sensors extensively through time, and transmits data on the Inter-net. This introduces problematic of battery consumption, which has not been quantified in this paper: as discussed in Section 7, we developed and exercised a prototype to verify the feasibility of the approach but a complete assessment of the solution through experimental evaluation is not reported. Also, the frequency of the acquisition of biometric data is fundamental for the protocol usage; if biometric data are acquired too much sparingly, the protocol would be basically useless. This mostly depends on the profile of the client and consequently on his usage of the device. Summarizing, battery consumption and user profile may constitute limitations to our approach, which in the worst case may require to narrow the applicability of the solution to specific cases, for example only when accessing specific web sites and for a limited time window, or to grant access to restricted areas.

6. Future Enhancement:

The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. The functions proposed for the evaluation of the session timeout are selected amongst a very large set of possible alternatives. The future work of this project is based on the detect the fake objects on the verification stage.

7. References:

1. Advanced .NET Remoting 2nd Edition (Ingo Rammer and Mario Szpuszta, Apress, Marc 2005) ISBN: 1-59059-417-7
2. Advanced .NET Remoting in VB.NET (Ingo Rammer, Apress, July 2002) ISBN: 978-1-59059-062-1
3. ASP to ASP.NET Migration Handbook (Christian Nagel et al, Wrox, and January 2003) ISBN: 978-1861008466
4. Beginning Visual C# (Christian Nagel et al, Wrox, and September 2001) ISBN: 1118314417
5. Data-Centric .NET Programming (Christian Nagel et al, Wrox, and December 2001) ISBN: 186100592X
6. Professional .NET Network Programming 2nd Edition (Christian Nagel et al, Wrox, and September 2004) ISBN: 1590593456
7. Professional C# (Christian Nagel et al, Wrox, and March 2002) ISBN: 1430242337. Professional C# Web Services (Christian Nagel et al, Wrox, and December 2001) ISBN: 1861004397
8. Microsoft Visual C# .NET 2003 Developer's Cookbook (Mark Schmidt, Christian Nagel, et al, SAMS, October 2003) ISBN: 0672325802