Securing Web Services by Iris Recognition System

Bava Elizabeth Mathew
MCA (M.Phil), Research Scholar
Department of Computer Applications
Karunya University
Coimbatore, India

ABSTRACT

A web service is defined as a software system designed to support interoperable machine-to-machine interaction over a network. It is an application programming interface. It can be published, located and invoked across the internet. As web service is connected to the internet, it is subjected to unauthorized intrusion. In order to ensure the availability, integrity and confidentiality of the web services, security is necessary. Access controls such as biometrics should be employed for the strong authentication. It is the most robust method to verify and identify an individual, once that person is properly enrolled. The bringing together of biometric and web services can strengthen both the technologies. Iris recognition system is a biometric method that has always held the promise of highly accurate identity verification, without compromising the simplicity of the web services. This paper describes how iris biometrics helps to secure web services.

Keywords- Authentication, Iris biometrics, Security, Unauthorized access, Web services

1. INTRODUCTION

In the past few years, ad hoc approaches have been used in business-to-business applications to take advantage of the basic internet infrastructure. The growth of internet technologies is revolutionizing the way organizations do business with their partners and customers. There have been three waves of internet development: e-mail, web sites and web services. E-mail and web sites have a profound socio-economic impact since e-mail enables people to communicate with each other and web sites helps people access to worldwide information. The latest development in using web for conducting business resulted in a new paradigm called web services. Web services made a promise to reiterate the success of its predecessors and it should allow applications to communicate and collaborate with each other without manual intervention [1].

Web services are evolving and gaining wide acceptance as a standard for distributed computing. Organizations are starting to rely on them to conduct their core business, thereby enabling access to a huge amount of sensitive personal, medical and financial information that they hold, as well as information held on behalf of their customers, such as governments. However, security for such web services is critical and security for web services is seen as a major challenge to be overcome before widespread deployment is possible [2]. Internet security breaches cause many problems to internet commerce. As web services are exposed to outer world, the security threat that exists in internet also affects the web services [3]. Biometrics can play an important role in web services in a number of ways, providing improved levels of security and convenience for end-users**.** Biometric technologies continue to advance, with growing impetus behind the establishment of common standards for distributed biometric systems [2].

2. WEB SERVICE AND SECURITY

Web services are software components, based on loosely coupled, distributed and independent services operating via the web infrastructure. Web services are platform and language independent, which is suitable for accessing them from heterogeneous environments [4]. It is a technology that allows applications to communicate with each other in a platform- and programming language-independent manner. It makes application functionality available over the internet in a standardized, programmatic way. A common web service framework identifies specific functions that need to be addressed in order to achieve decentralized interoperability. Without a common framework and coordinated development of each component, the implementations will be more complex and decrease the probability of achieving interoperability. The framework also allows the development and adoption of the individual components to happen in parallel and asynchronously. The web services framework (Figure.1) is divided into three areas

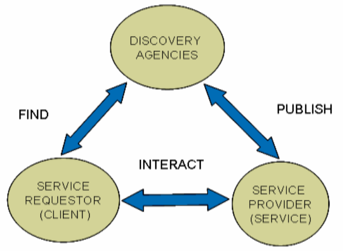


Figure 1 Web service framework

- Communication protocols - Simple Object Access Protocol (SOAP) that enables communications among web services
- Service descriptions - Web Services Description Language (WSDL) that provides a formal, computer-readable description of web services
- Service discovery - Universal Description, Discovery and Integration (UDDI) directory that is a registry of web services descriptions

Web services can be accessed and invoked via standards such as XML, WSDL, UDDI and SOAP. SOAP is fundamentally a stateless, one-way message exchange paradigm that enables applications to create more complex interaction patterns by combining one-way exchanges with features provided by an underlying protocol and/or application-specific information [5]. A WSDL abstractly describes messages and operations [6]. WSDL provides a model and an XML format for describing Web services. It is a document that describes the service's location on the web and the functionality the service provides. UDDI provides a mechanism for clients to find Web services [7]. Information related to the web service is to be entered in a UDDI registry, which permits web service consumers to find out and locate the services they required. Using the information available in the UDDI registry based on the web services, client developer uses instructions in the WSDL to construct SOAP messages for exchanging data with the service over HTTP attributes [8].

SOAP, WSDL, and UDDI are important technologies to enable web services. However, to fully satisfy the requirements of business applications, the current technologies have shortcomings, which affect the security of web service. None of components of the web services such as XML, SOAP, WSDL, or UDDI directly implements security or provide solution to security threats [9]. Basically, the security problems that are likely to affect web services are the same as those that have affected the conventional web-based systems. In the web services context, security means that the recipient of a message should be able to verify the integrity of the message and to make sure that it has not been modified. The recipient should have received a message confidentially so that unauthorized users could not read it, know the identity of the sender and determine whether or not the centre is authorized to carry out the operation requested in the message [5]. There are five key threats to the security of Web services, which are given below:

- Unauthorized access - refers when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner
- Parameter manipulation - refers to the unauthorized modification of data sent between the web service consumer and the web service
- Network eavesdropping -an attacker is able to view web service messages as they flow across the network
- Disclosure of configuration data - refers to the revealing of the information to the attacker
- Message replay - an attacker captures and copies a message and replays it to the web service impersonating the client. The message may or may not be modified [10]

Among the five major security threats mentioned above, unauthorized access will be focused which comes under the unauthorized activities. Unauthorized access focuses on the accessing of personal information by unauthorized parties. Another closely related area is the excessive access of personal information by authorized parties [11]. Access to information system i.e. data or information is secured through the proper authentication and authorization. Authentication of an entity, provided by web services security, is usually done by verifying one or more of the followings:

- Something the entity is (by *biometric* techniques)
- Something the entity has (by PKI certificate, IDcards, smart cards)
- Something the entity knows (by passwords) [12].

3. IRIS RECOGNITION SYSTEM

The weakest link in secure system design is user authentication. Biometrics can strengthen this weakness [13]. A biometric has been defined as a measurable, physical characteristic or personal behavioural trait that can be used to recognize the identity, or verify the claimed identity, of an enrollee [14]. Biometrics is the science of measuring human characteristics that are stable and unique among individuals. Biometric characteristics can be divided in two main classes. Physiological are related to the external characteristics of the body and e.g. are fingerprint, face recognition, hand geometry, iris recognition. Behavioural characteristics include typing rhythm, gait, and voice.

Considerations of reliability and invasiveness suggest that the human iris (Figure. 2) is a particularly interesting structure on which to base a biometric approach for personnel verification and identification. . Owing to the features like reliability and non invasiveness, iris recognition is a promising approach to biometric based verification and identification of people [15]. In recent years, iris recognition has become the major recognition technology since it is the most reliable form of biometrics. The future of the iris recognition system is better in fields that demands rapid identification of the individuals in a dynamic environment [16].

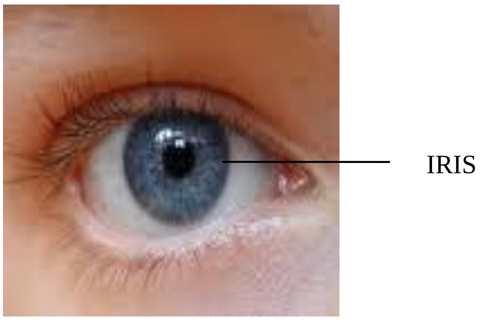


Figure 2 Picture of an iris

3.1 Iris recognition system process

In general, the process of iris recognition system consists of:

- *Image acquisition*: An important and difficult step of an iris recognition system is image acquisition. In this step, an image containing the user's eye is captured by the system [17].
- *Preprocessing the iris image*: The acquired image always contains not only the 'useful' parts (iris) but also some 'irrelevant' parts (e.g. eyelid, pupil etc.). Under some conditions, the brightness is not uniformly distributed. In addition, different eye-to camera distance may result in different image sizes of the same eye. For the purpose of analysis, the original image needs to be preprocessed. The preprocessing is composed of three steps and they are iris localization or segmentation, normalization and image enhancement. Here the image is preprocessed to normalize the scale and illumination of the iris and localize the iris in the image [15]. Localization of the iris is an important step in iris recognition system because if it done improperly, the resultant disturbance in the image may lead to poor performance. It is used to identify the boundaries of iris

and pupil as circles. In the normalization, the localized image is converted to rectangular block image. The original iris image has low contrast and may have non-uniform illumination caused by the position of the light source. These may impair the result of the texture analysis. So the image has to be enhanced.

- *Iris feature extraction*: In iris feature extraction or encoding, features representing the iris patterns are extracted. For this purpose a well-established texture analysis method to extract features from the normalized block of texture image, namely wavelet transform is used. Wavelet transform is a good scale analysis tool and has been used for texture discrimination [18].

- *Iris matching:* In the last step iris matching or identification, the authentication decision is made. In this process, it determines how closely the produced code matches the encoded features stored in the database. For this process, Hamming distance is the used, in which two iris codes are compared. Hamming distance will be the number of corresponding bits that differ between the two iris codes. [15].

4. INTEGRATING IRIS RECOGNITION SYSTEM WITH WEB SERVICES

In the Figure. 3 given below, first the user's iris image is captured and then it is preprocessed, undergoing localization, normalization and enhancement. After the preprocessing the image, encoding or extraction is done, in order to produce fine features of iris containing binary iris code, creating a template.

A template that contains only a user's biometric data will be of limited use in a distributed biometric system. CBEFF (Common Biometric Exchange File Format) defines a basic structure for biometric data, facilitating exchange of biometric information between systems. XCBF (XML Common Biometric Format) defines a set of XML encodings for patron formats defined by CBEFF. Organisations that have developed CBEFF conformant biometric systems are known as *Patrons.* The main advantage of encoding biometric data in XML is that the data is represented in a format that is readable and extremely flexible. The XCBF data can then be sent along with a web service request, using the WS Security standard to add the biometric data in the SOAP message [2]. The resultant template is stored in the database.

Finally, in the matching process generates a match score by comparing the feature sets of two iris codes templates. During the verification process, data extracted from the biometric sample is compared to enrolled templates. The technique used for comparing two iris codes is the Hamming distance, which is the number of corresponding bits that differ between the two iris codes [16]. Based on the resultant match score, user is authenticated for accessing the web service. As with the storage of templates, the storage of policies containing access rights must be carefully designed. Furthermore, the process of enforcing these policies via the user interface (UI) must also be secured, to avoid introducing further vulnerabilities [13].

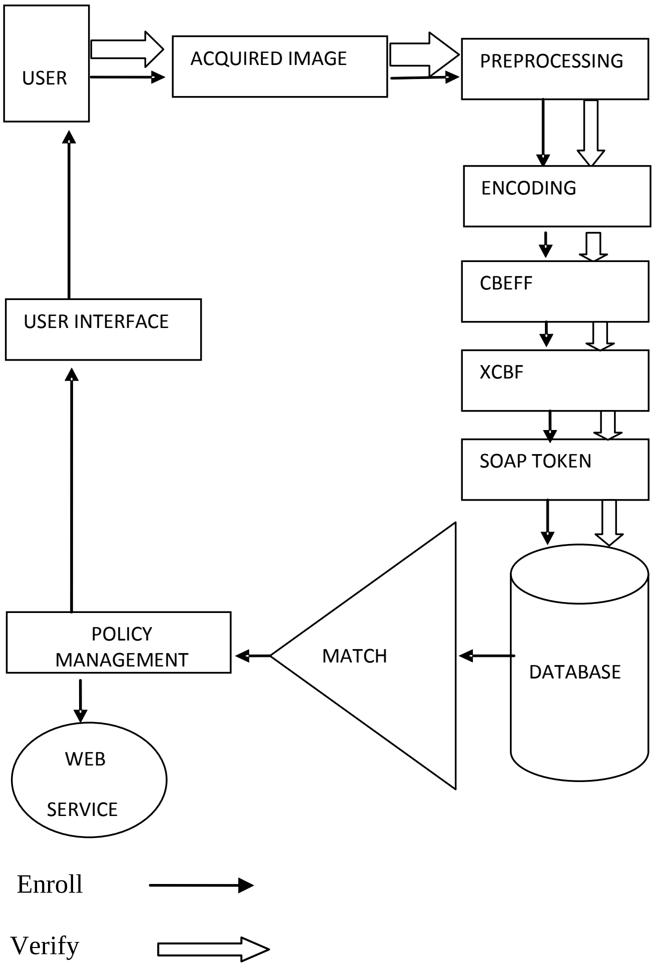


Figure 3 Iris biomterics enabled web services

5. RESULT

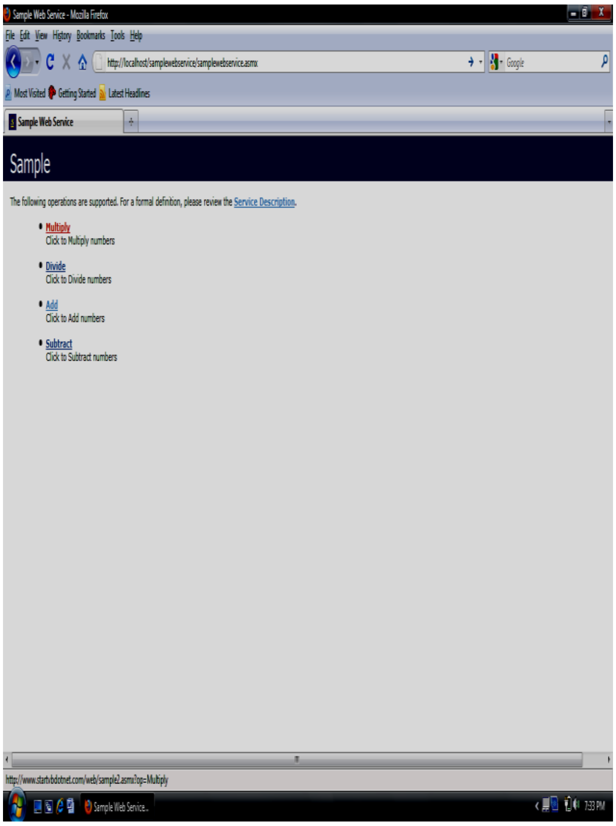
In the first process of iris recognition system, image has to be acquired. Devices like scanners and cameras can be used in image acquisition process. Near infrared is used for illumination. The test data i.e. iris images used in this process are grayscale. The acquired image is localized and then normalized. The normalized image is displayed as a rectangular image with the radical coordinate on the vertical axis and angular coordinate on the horizontal axis. In this image, the pupil boundary will be on the top. A simple deviation or the tilt of the head can affect the angular coordinates. The normalized image is enhanced (Figure.4). The enhanced image is extracted or encoded (Figure.5)

Figure 4 Enhanced im

1 1 1 1 1 1 1 0 1 0 1 0 1 0 0 0 0 0

Figure 5 Encoded feature

The encoded binary code is embedded in XCBF (Table 1) and then the encoded binary code will be compared with the enrolled code during the verification process through the Hamming distance. The Hamming distance is the number of bits that disagree. During the matching process, hamming distance compares the presented binary code and referenced or enrolled binary code. If number of bits in each code differs by position, it gives a numeric count of 1 otherwise it gives 0 i.e. If the binary codes are equal, a numeric value of 0 will be presented indicating a positive authentication and user get access to the given web service (Figure.6). Otherwise a numeric value of 1 will be generated indicating denied access. If the access is granted or denied, then the user will be acknowledged through the user interface.


Sample Web Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/samplewebservice/samplewebservice.asmx
Google
Most Visited
Getting Started
Latest Headlines
Sample Web Service
http://www.startvbdotnet.com/web/sample2.asmx?op=Multiply
Sample Web Service...
7:33 PM

Sample

The following operations are supported. For a formal definition, please review the Service Description.

- Multiply
  Click to Multiply numbers
- Divide
  Click to Divide numbers
- Add
  Click to Add numbers
- Subtract
  Click to Subtract numbers

Figure 6 Web Service

6. CONCLUSION

In this paper, the analysis of the need of security in the web services and the usage of iris biometrics for the strong authentication is presented. The aim of this work is to integrate iris recognition biometric system with the web service for the authentication purpose.

As iris recognition system is unique and accurate, it is used mainly for the authentication purpose. The usage is simple and non intrusive for the users. It also speeds up the verification and identification functions within limited time. While the most common use of iris recognition to date is physical access control in private and government enterprise, the versatility of the technology will lead to its growing use in large sectors of the economy such as banking, transportation, healthcare, and national identification programs. Although security is clearly a prime concern, iris recognition is also being adopted for productivity-enhancing applications like time and attendance. By using web services as a means for interoperability, the capabilities and reach of biometrics is significantly improved. Having a web services-based biometric device interface helps to establish multimodal biometrics, improve biometric sensor acquisition and *e*nable mobile biometrics

Table 1 XCBF Security Code

```
<S:Header>
<wsse:Security xmlns:wsse="...">
<wsse:XCBFSecurityToken
  Id="XCBF-biometric-object"
 ValueType="wsse:XCBFv1"
 EncodingType="wsee:XER">
<BiometricSyntaxSets>
<BiometricSyntax>
<biometricObjects>
<BiometricObject>
<biometricHeader>
<version> 0 </version>
<recordType> <id> 8 </id> </recordType>
<dataType> <intermediate/> </dataType>
<purpose> <enrollIdentify/> </purpose>
<quality> 100 </quality>
<validityPeriod>
<notBefore> 1990.10.4 </notBefore>
<notAfter>2011.10.3.23.59.59</notAfter>
</validityPeriod>
<format>
<formatOwner>
<oid> 2.23.42.9.10.4.2 </oid>
</formatOwner>
</format>
</biometricHeader>
<biometricData>
  111111101010100000
</biometricData>
</BiometricObject>
</biometricObjects>
</BiometricSyntax>
</BiometricSyntaxSets>
</wsse:XCBFSecurityToken>
</wsse:Security>
</S:Header>
```

7. REFERENCES

[1] A. Tsalgatidou, T. Pilioura, “An Overview of Standards and Related Technology in Web Services”, International Journal of Distributed and Parallel Databases, Special Issue on E-Services, 12(2) Sep 2002, pp. 135-162.

[1] Luann Rragami, Nicholas H. Edwards, "Securing web services with biometrics", Biometric Technology Today, 11 (5) (2003), pp. 6-8

[2] David C.Chou, Kirill Yurov, "Security development in web services environment ", Computer standards and interfaces , 27 (3) (2005), pp. 233-240.

[3] Ramakanta Mohanty, V. Ravi b, M.R. Patra , "Web-services classification using intelligent techniques", Expert Systems with Applications ,37 (2010), pp. 5484–5490.

[4] Hongbing Wang, Joshua Zhexue Huang, Yuzhong Qu and Junyuan Xie, "Web services: problems and future directions", Journal of web semantics 1 (2004), pp. 309-320.

[5] Christian Geuer-Pollmann, Joris Claessens, "Web services and web service security standards", Information Security Technical Report 10 (2005), pp 15-24.

[6] UDDI. Version 3.0, <http://uddi.org/pubs/uddi-v3.00-published-20020719.htm > , 19 July 2002

[7] Kokash," Web service discovery with implicit QoS filtering", In Proceedings of the IBM PhD student symposium, in conjunction with ICSOC'05, pp. 61–66, Netherlands.

[8] Weaver et al., "Federated, secure trust networks for distributed healthcare IT services", Industrial Informatics, 2004, pp. 162 – 169.

[9] Stuart King, "Threat and solutions to web service security", Network Security, 9(2003), pp. 8-11.

[10] Rasika Dayarathna, "The principle of safety safeguards: unauthorized activities", Computer Law and Security Review, 25 (2009) , pp. 165-172.

[11] Mohamed G. Gouda, Alex X. Liu, Lok M. Leung, Mohamed A. Alam," SPP: An anti phishing single password protocol", Computer Networks, 51 (2007), pp. 3715–3726.

[12] J. Wayman, A. Jain, D. Maltoni, D. Maio, Biometric Systems, Technology, Design and Performance Evaluation, 2005

[13] Marek Rejman-Green**,** **"**Secure authentication using biometric methods"**,** Information Security Technical Report, 7 (3) (2002), pp. 30-40

[14] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification system based on iris pattern" ChinesePatent Application, No. 9911025.6, 1999

[15] Arun Ross, "Iris recognition: the path forward", IEEE Computer Society, 2010.

[16] Makram Nabti, Ahmed Bouridane, "An effective and fast iris recognition system based on a combined multiscale feature extraction technique", Pattern Recognition, 41 (2008), pp. 868 – 879.

[17] Laine and J. Fan, "Texture classification by wavelet packet signatures", IEEE Trans. Pattern Anal. Machine Intell., vol.15, 1993,pp.1186-1191.