Volume 2, No. 4, April 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

DEFENDING AGAINST ATTACKS BY ENHANCING SECURITY USING BIOMETRICS IN SEMANTIC WEB

Mr. Akhilesh Dwivedi[*1], Mr. Suresh Kumar[2]

[*1]M.Tech (Information Security) Scholar, Department of Computer Science and Engineering,
Ambedkar Institute of Technology, Govt. of NCT Delhi, Geeta Colony, New Delhi, India
dwivedian5@gmail.com[1]

[2]Assistant Professor, Department of Computer Science and Engineering,
Ambedkar Institute of Technology, Govt. of NCT Delhi, Geeta Colony, New Delhi, India
sureshpoonia@yahoo.com[2]

Abstract: Semantic Web is maturing day by day and data and information integration is growing and becoming crucial. Security is one of the key features of the future Internet's security. So it is necessary harnessing the synergy in biometrics and in Semantic Web. It can leverage the lack of widely accepted biometrics security standards along with Semantic Web technologies to protect, represent, store and query metadata and data across biometrics datasets. However, the success of security mostly relies on user profiles. Therefore, a biometric user profile is crucial for service providers for the uptake of security services of Semantic Web. Biometric systems provide the solution to ensure that the rendered services are accessed only by a legitimate user and no one else. The security is dependent on the secrecy trustworthiness of the authentication because deeper the trust level of authenticator, stronger will be security of Semantic Web.

Keywords: Attacks, Authentication, Authorization, Biometrics, Semantic Web, Security, Trustworthiness, Federation

I. INTRODUCTION

The Future Internet provides a powerful, standardized, world-wide, ubiquitous communications mechanism whose benefits are impossible to ignore [1]. We think that Internet-accessible information is the clear wave of the future, provided that such access is reliable, dependable, and authentic. The Semantic Web Services community has already made great strides in defining the framework, standards, and languages needed for Semantic Web Service interactions. As promoted by the World Wide Web Consortium (W3C) [2], Semantic Web services are now seen as the preferential way to link applications both within and without an organization in a loosely-coupled, language-neutral, platform-independent way. A Semantic Web Services approach enables designing, publishing, promoting, registering, and initiating processes dynamically in a distributed computing environment. The Semantic Web is about adding machine-understandable and machine-process able metadata to Semantic Web resources through its key enabling technology i.e. ontology [3]. Ontology is a formal, explicit and shared specification of conceptualization. The goal of the Semantic Web is to provide a response to the ever-growing need for secure data integration on the Semantic Web meanwhile research in biometrics is focused on strategies and techniques for uniquely recognizing humans based upon one or more intrinsic traits i.e. physical or behavioral. Particularly, biometric authentication refers to technologies to analyze and measure such traits for authentication purposes [4]. Nevertheless, such technologies are data intensive and prone to generate massive amount of information about biometric identities, pertaining large scale data repositories of biometric features which are usually shared and transmitted through the Semantic Web. As discussed in [5], bridging biometrics with Semantic Web would permit to organize properly data fostering analysis and access of such information to accomplish critical tasks such as processing biometrics data to study. The need of adding biometrics to the Semantic Web and use Semantics to achieve information integration becomes even more critical as information systems become more complicate and data formats gain a more complex structure. Particularly in those fields where massive data gathering is faced, the need of information integration is critical, preserving by all means the Semantics inherent to the different data sources and formats. The benefit of adding biometrics in Semantic Web is to provide empowerment and more security to Semantic Web. In this paper, we present our approach for defending against attacks and enhancing security using biometrics in Semantic Web. This paper proposes a user-centric biometric approach to increase the depth of trust of Semantic Web security.

II. SEMANTIC WEB THE FUTURE INTERNET

The Semantic Web term was coined in [5] to describe the evolution of a Web that consisted largely of documents for humans to read towards a new paradigm that included data and information for computers to manipulate. The Semantic Web will provide an infrastructure that enables not just web pages, but databases, services, programs, sensors, personal devices, and even household appliances to both consume and produce data on the web [23]. Ontologies [3] are its cornerstone technology, providing structured vocabularies that describe a formal specification of a shared conceptualization. The fundamental aim of the Semantic Web is to provide a response to the ever-growing need for

data integration on the Web. Semantics can be achieved by formally capturing the meaning of data, since a common data format will likely never be achieved, eventually leading to efficiently managing data by establishing a common understanding. The Semantic Web standard ontology language is OWL (Web Ontology Language) [3]. OWL is a markup language for publishing and sharing data using ontologies on the Internet. OWL is a vocabulary extension of the Resource Description Framework (RDF) and is derived from the DAML+OIL Web Ontology Language. The OWL specification is maintained by the World Wide Web Consortium (W3C) [2].

A more lightweight ontology language is the Resource Description Framework (RDF) [3]. RDF is a family of specifications for a metadata model that is often implemented as an application of XML. The RDF family of specifications is maintained by the World Wide Web Consortium (W3C). The RDF metadata model is based upon the idea of making statements about resources in the form of a subject-predicate object expression, called a triple in RDF terminology. The subject is the resource, the "thing" being described. The predicate is a trait or aspect about that resource, and often expresses a relationship between the subject and the object. The object is the object of the relationship or value of that trait. The RDF simple data model and ability to model disparate, abstract concepts has also led to its increasing use in knowledge management applications unrelated to Semantic Web activity. Key applications of semantic web [23, 24] are e-banking [29], e-learning [30], e-commerce [31], Semantic Search [24], Bioinformatics [27], Knowledge Management [28], Semantic based Enterprise application and data integration [25], Knowledge Base [26] etc. these areas of application requires a high level of security. So we need to focus on the future internet's key security issues and considerations. The next section elaborates it and proposes our novel framework in this regard.

III. THE FUTURE INTERNET'S KEY SECURITY ISSUES AND CONSIDERATIONS

The Security is dependent on the secrecy, trustworthiness of the authenticators (password, PIN, e-token, biometrics) because deeper the trust level of authenticator, stronger will be security. But it would clearly not be feasible to remember the user authentication based on so much big key every time. Here a novel framework is presented where the user is not bothered to remember any key every time because his/ her biometrics traits will work as authentication key. The biometrics traits e.g. fingerprint, hand, eye, face, and voice, keystroke dynamics encrypt with original message to generate the encrypted data and further the same will be used to decrypt it. Each Semantic Web Service specifies its authentication and authorization policies using Standard Semantic Web Service Policy combined with our valuable framework's concepts of trust levels and trust level mappings across domains. Biometric authentication Web service verifies human identities via biometrics are vetted by digital signatures. Biometric authorization Web service enforces a dynamic, context-aware access policy. Biometric Trust Federation is used to manage trust relationships across separate but cooperating trust domains. The theme for Secure Intelligent Semantic Web is the exchange of code and data in a uniform and verifiable way. When either a human or a software application requests process data for purposes of monitoring or control, and likewise whenever any software is installed, there is the risk of a security breach and the more distributed Web, the more difficult it is to guarantee the integrity of the overall system. The human could be an imposter and the software upgrade could contain a virus.

To achieve the key objectives of security enhancement using biometrics in Semantic Web we have proposed our novel framework in two parts i.e. Level1 (L1) and Level2 (L2) which is categorised below and each of below is explained in next sections separately.

Level-1 framework (L1) for security enhancement using biometric authentication in semantic web

Biometric Authentication: – who is making the request?
Biometric Authentication trust level: – what is the reliability of the user's identification?

Level-2 framework (L2) for security enhancement using biometric authorization in semantic web

Biometric Authorization: – is this user permitted to read, write, change, or delete this data?
Biometric Trust for Semantic Web Federation: – how can identity, once legitimately established in one system, be safely exported to another cooperating system?

IV. LEVEL-1 FRAMEWORK (L1) FOR SECURITY ENHANCEMENT USING BIOMETRIC AUTHENTICATION IN SEMANTIC WEB

Framework shown in figure-1 is a block diagram use to represent component that participate in communication. There are two entity service provider and service consumer. Clients are service consumers and publishers are service provider (SP). Web servers are a resource where provider can upload services and get acknowledgement about successful uploading. Now provider assures about published service to make accessible for clients on internet [6].

Client

Clients are entities, who are availing these published services from Web server. Some of them may be freely available other may chargeable. Freely available services are not so much vulnerable as financial services, like net banking, e-transaction, e-money exchange are more vulnerable rather than chatting, instant messaging etc . Client is a consumer of services running on Semantic Web server.

Semantic Web Server

Semantic Web Server is common, distributed platform to fetch data and retrieve data by using Semantic Web services throughout internet. Web servers are internet connected system who responds all coming request from client side. These servers continuously run Web services for which they are designed.

Service Provider

Service providers are organizations are trusted third party like bank, health care or any government institutions those publish their Web services on Semantic Web server that is a

part of Semantic Web. These Web services can be do some work on behalf of user, like automation of maximum manual works in insurance, banking, brokering etc [5].

Semantic Web Services

They are self-contained, self describing, modular applications that can be published, located, and invoked across the Web. Web services perform functions, which can be anything from simple requests to complicated business processes. "Once a Web service is deployed on server applications or other Web services can discover and invoke all those service" [7].

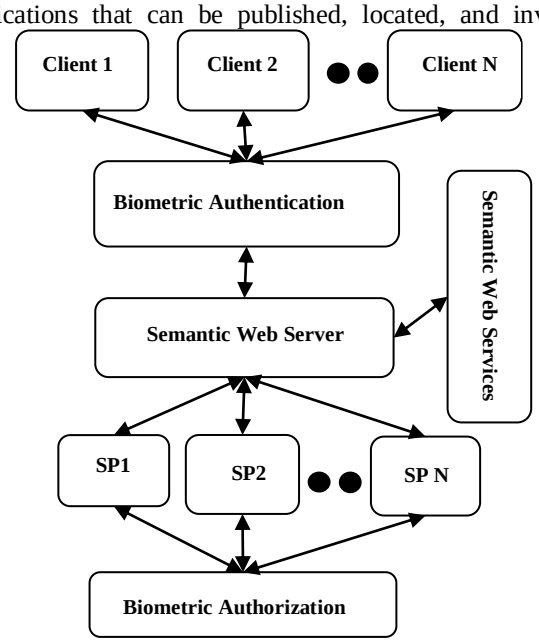

Figure 1. Level-1framework(L1) for security enhancement using biometric authentication in semantic web

Biometric Authentication

It is important to note that biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as e-commerce [13]. It is well known that for software applications, authentication is provided via digital signatures. For individuals, the Semantic Web portal can support both biometric and other digital techniques. For biometrics ("who you are"), we have currently shown in Figure 3(a), the enrollment of templates into authentication database of Semantic Web. Which works on the principal that who you are? And do support that you are you. Various types of scanners are available for different types of purposes of enrollment of templates in database. The RSA SecurID [32] system requires a password ("what you know") plus the correct random number at the moment of login ("what you have"). Figure 3(b) shows validation process for enrolled biometric data from authentication database of Semantic Web.

Biometrics Authentication Trust Levels

We have proposed Semantic Web Service Policy and SWS-Security Policy to support our novel concepts of biometric authentication trust levels, biometrics trust for federation, and trust mapping within the Semantic Web services architecture. We have defined a generic format for all authentication tokens that includes the concept of trust level that is, a numeric representation of the underlying reliability of the authentication technology. This allows the Semantic Web service to support an authentication policy such as "authentication requires a trust level of fingerprint or higher." The current SWS-Policy implementation in SWSE supports simple authentication policies such as "require an X.509 certificate" or "require a Kerberos ticket", "PKI" [8, 22]. By using our novel concept of biometrics authorization engine, we can enforce custom policies such as "require authentication from a wired device within the enterprise to be at the trust level of a password or a biometric identity, but access from any wireless device requires authentication at the level of a fingerprint or higher." A major advantage of our approach is that if identity has been previously established with a higher reliability technique, that higher-trust authentication token can be used as a substitute for a required lower-reliability one without forcing the user to undergo a secondary authentication procedure.

Setting biometrics authentication trust levels: The utility of this more general scheme that accepts tokens based upon trust level (while still permitting static enumeration of specific acceptable technologies, as is currently done) depends upon having an agreement about the trust level T() to be associated with any particular biometric authentication technique. In the abstract, trust levels are ordered based upon the number of degrees of freedom inherent to the underlying identification technology. For example, there is general agreement that *T (multimodal) >.....>T (retina) > T (iris) > T (fingerprint) > T (password).* In practice, the trust level of any specific product must be determined by experimentation to quantify its false acceptance and false rejection rates (the false acceptance rate is the percentage of authentication attempts by a person other than the enrolled individual which are nevertheless successful; the false rejection rate is the percentage of authentication attempts by the enrolled individual which are nevertheless rejected). Figure 2 shows biometric system error rates and relation between FAR or FMR and FRR or FNMR. Setting the trust levels for differing authentication technologies in the local trust domain is straightforward and no more difficult than current practice. Systems administrators already make decisions about which technologies they trust, and how much. However, if the authentication extends beyond the local trust domain, then we need trust authorities that can mediate the assignment of trust levels; for that, *biometric trust for Semantic Web federation* is required (see L2 framework).

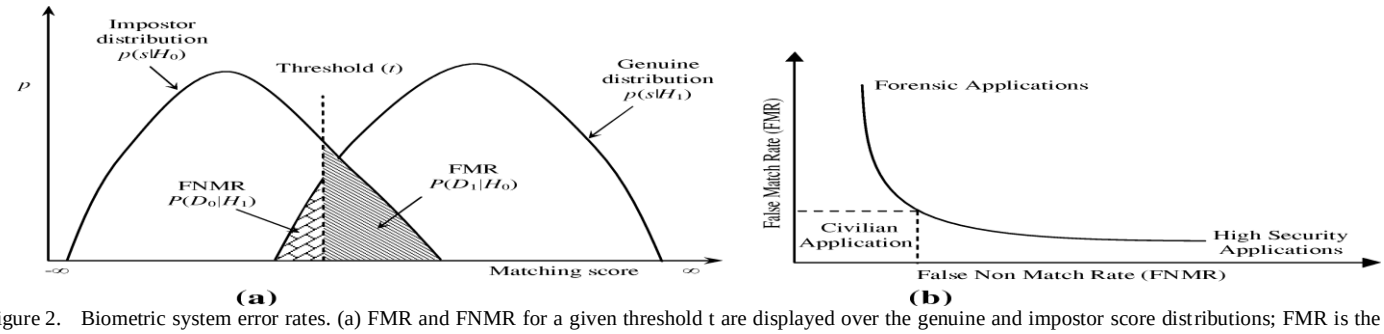

Figure 2. Biometric system error rates. (a) FMR and FNMR for a given threshold t are displayed over the genuine and impostor score distributions; FMR is the percentage of non-mate pairs whose matching scores are greater than or equal to t, and FNMR is the percentage of mate pairs whose matching scores are less than t. (b) Choosing different operating points results in different FMR and FNMR. The curve relating FMR to FNMR at different thresholds is referred to as receiver operating characteristics (ROC). Typical operating points of different biometric applications are displayed on an ROC curve. Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor/user communities a like [15].

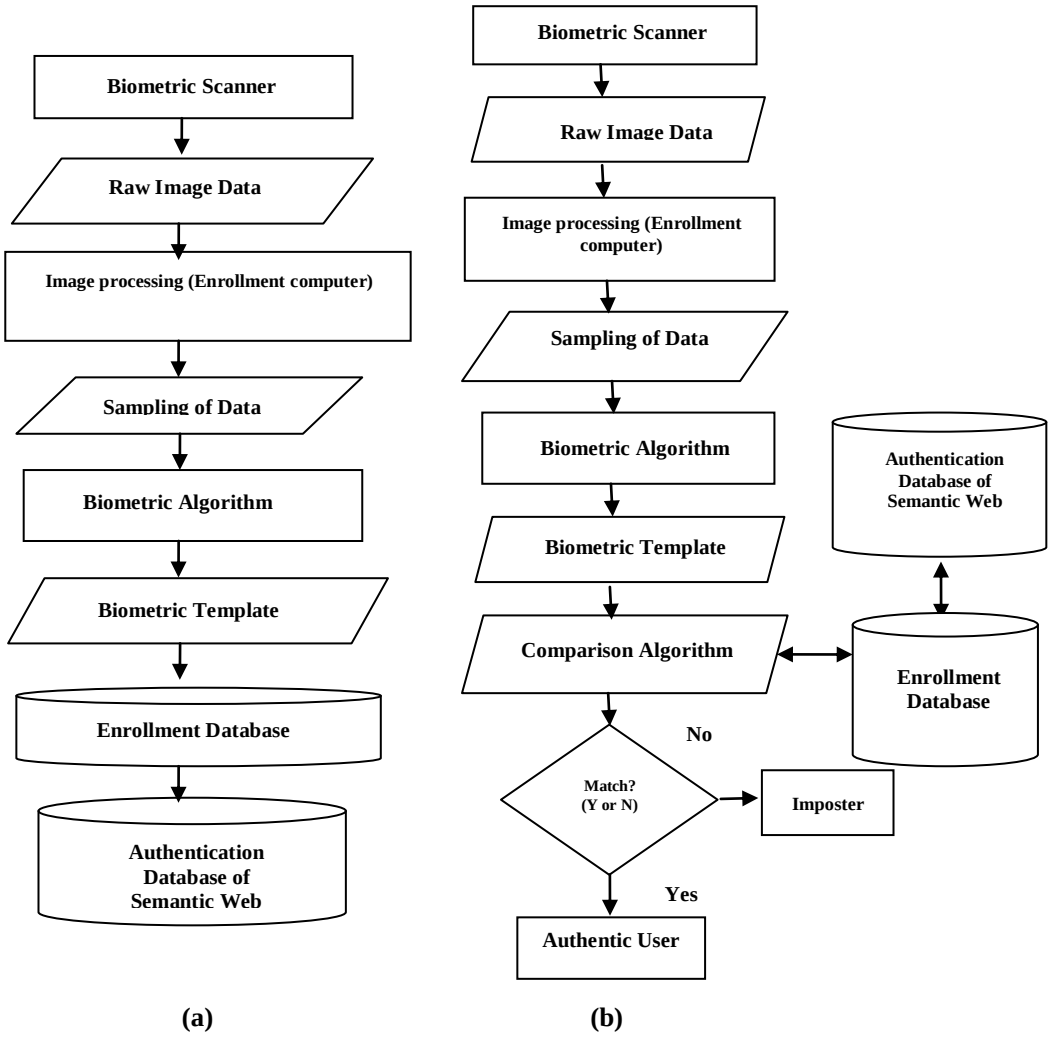

Figure 3. Biometric enrollment and validation: (a) Enrollment of biometric data into authentication database of Semantic Web, (b) Validation process for enrolled biometric data (template) from authentication database of Semantic Web.

V. LEVEL-2 FRAMEWORK (L2) FOR SECURITY ENHANCEMENT USING BIOMETRIC AUTHORIZATION IN SEMANTIC WEB

Figure 4 is level-2 diagram use to represent detail communication between main components of Semantic Web. Semantic Web service describes a work flow or processing steps to complete a task. Client communicates with Web service facilitator. Web service facilitator annotates that particular Web services and upload it on server's directory. If any client want to access that particular service, then client request to facilitator. Web server maintains all description of Web services in WSDL Web service description language. OWL is Web ontology language use to design meaning with help of RDF and XML Metadata description language. SAML is also used to enforce security assertion, logical reasoning [10].

Facility Descriptor

Facility descriptor checks coming request from clients to serve according to categories, this is an interface between Web server and client. Facilitator knows well about services running in UDDI directory. When client requests for a service from Web server, facilitator categories request to be serve better way. Facility descriptor play vital role to access, describe, upload services on Web. There must be a secure communication between these basic components of Semantic Web technologies. Clint and provider both need to authentication and validation before they are either uploading services on server [12].

OWL

Ontology Web language are use to describe ontology. Ontology typically consists of a hierarchical description of important concepts in a domain or community, along with descriptions of the properties of instances. OWL (like DAML+OIL) is largely based on a Description Logic [1]. OWL currently has three flavors: OWL Lite, OWL DL, and OWL Full. These flavors incorporate different features, and in general it is easier to reason about OWL Lite than OWL DL and OWL DL than OWL Full. OWL Lite and OWL DL are constructed in such a way that every statement can be decided in finite time; OWL Full can contain endless 'loops'. OWL DL is based on description logics. Its subset OWL Lite is based on less expressive logic. OWL Lite supports those users primarily needing a classification hierarchy and simple constraints. For example, while it supports cardinality constraints, it only permits cardinality values of 0 or 1. OWL DL supports those users who want the maximum expressiveness while retaining computational completeness (all conclusions are guaranteed to be computed) and decidability (all computations will finish in finite time). Finally, OWL Full is meant for users who want maximum expressiveness and the syntactic freedom of RDF with no computational guarantees. For example, in OWL Full a class can be treated simultaneously as a collection of individuals and as an individual in its own right. OWL Full allows an ontology to augment the meaning of the pre-defined (RDF or OWL) vocabulary. It is unlikely that any reasoning software will be able to support complete reasoning for every feature of OWL Full [3].

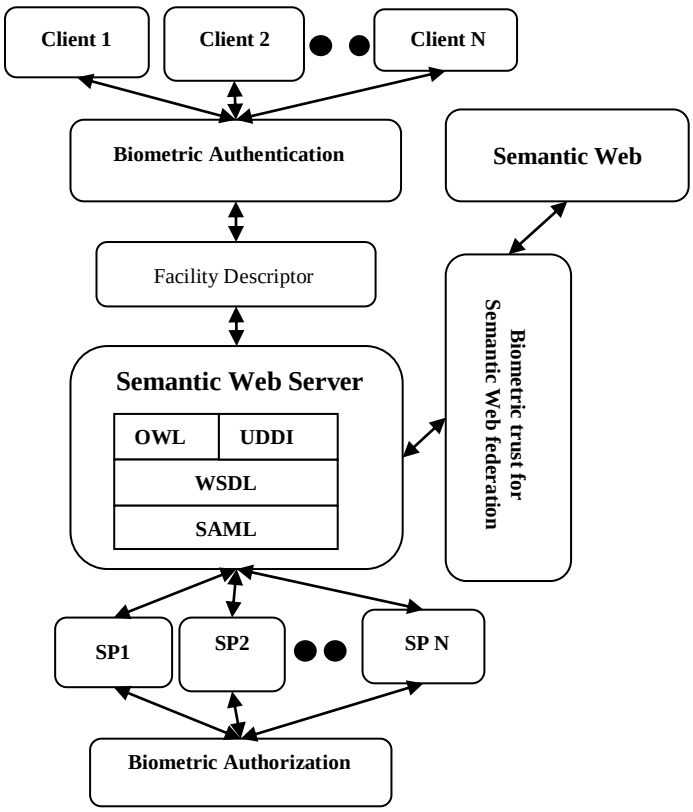

Figure 4. Level-2framework(L2) for security enhancement using biometric authorization in semantic web

UDDI

UDDI is stands for Universal Description, Discovery and Integration. UDDI serves as a "Business and services" registry and directory and are essential for dynamic usage of Web services [33]. A UDDI registry is similar to a CORBA trader or it can be thought of as a DNS for business applications. It is a platform independent framework for describing services, discovering businesses, and integrating business services by using the Internet.

WSDL

WSDL defines services as collections of network endpoints or ports. A port is defined by associating a network address with a binding; a collection of ports define a service. WSDL stands for "Web Services Description Language". WSDL is an XML document. WSDL is used to describe Web services. WSDL is also used to locate Web services [1].

SAML

SAML statements are called assertions. They are XML constructions and have a nested structure, represented as whereby a single assertion might contain several different information items referring to authentication, authorization decisions, and attributes such as credentials or group membership designator [11].

Biometric Authorization

In the conventional role-based access control (RBAC) model [9], a typical authorization policy is represented as "User U in role R has permission P." However, to make our access control infrastructure aware of context information, it is necessary to define context-related constraints in authorization policies. We will permit access policies such as "User U with identity I in role R who satisfies constraint

C has permission P." Here, a constraint is defined as a restriction that can be applied by the authorization policy: permission P is granted to role R with identity I if and only if constraint C is satisfied. Numerous types of contexts are possible, but we are mainly concerned with the context of the current access request (e.g., the status of the user making a request; the status of the object being requested; when and where the request originated). By adding context-based constraints to the authorization policy, authorization can be determined dynamically based upon the current context of the request, rather than just the role of the user.

Biometric Trust for Semantic Web Federation

Biometric Federation will be a collection of realms or domains that will have established trust for biometric identity. As a real life example, consider the case of using one bank's debit card in another bank's ATM. The networking and security infrastructure will determine whether the identity established at bank X is sufficiently reliable for acceptance at bank Y. Biometric Federated Systems will operate across organizational and technical boundaries, including different operating systems and different security platforms. Biometric Federation will depend upon two authorities being resident in each domain.

Biometric Security Token Service (BSTS): A Semantic Web Service that will issue biometric security tokens will make assertions to whomever trust based upon evidence that BSTS will trust itself.

Biometric Identity Provider (BIP: This entity will act as a biometric authentication service to end requestors, and will be an extension of a basic BSTS Service.

Because trust domains (loan, money exchange, insurance etc) will be independently established and maintained, biometric federation will address different trust topologies; it will model existing business practices and at the same time will leverage existing infrastructure. As an example, suppose that a user has legitimately established his identity and received a biometric authentication token within the organization (for e.g. bank) trust domain. If the user now wishes to access data at a different but cooperating (for e.g. loan, insurance, money exchange) facility, how can the trust established in the organization trust domain be exported to the other trust domain? See Figure 5 (arrow (9) and (10)). We find three solutions for this problem of biometric trust for semantic web federation:

Biometric Security Token Exchange: Alternatively, if system X will want to make a service request of system Y, and if system X's BSTS trusts system Y's BSTS, then system Y will issue an access token valid in system Y (an exchange token) based upon its trust of the system X BSTS's assertion that identity will have been satisfactorily established within system X.

Biometric Security Token Validation: System X will make a service request of system Y. If the two BSTSs will be trusted by each other, then the system X BSTS will provide the local identity token (other than biometric for e.g. a random number or pass code) that it will create and will certify its validity; the system Y BSTS will then certify the local identify token from system X for use in system Y.

Indirect Trust: The more general solution would be borrowed from the schemes used for validating digital signatures using certification authorities. In this case, system X's BSTS will be trust a known set of other STSs (other than biometric for e.g. a random number or a RFID token, password etc), and system Y's BSTS will be trust any of these known set of STSs. If the trust set of system X will have a member in common with the trust set of system Y, then that common member in the two trust groups will validate the security tokens of each system to the other. The common member's STS then will certify identity tokens originating in system X to STS Y and vice versa. Another consideration is that the trust level definitions of one domain may not be consistent with those of a separate and independent domain. For that reason we will have to provide a mapping function that will allow a system administrator to map the trust levels of one domain into those of another. The next section focuses a light on biometric security infrastructure for semantic web which shows the increase in depth of trust than other authenticators (password, e-tokens) by using biometrics infrastructure for Semantic Web and its applications as shown in Figure 5.

VI. BIOMETRIC SECURITY INFRASTRUCTURE FOR SEMANTIC WEB

As illustrated in figure 5, a user interface is used to access the organization's Semantic Web portal and display real-time process parameters; data values are retrieved from the organization's data repository using Semantic Web Services. How do we know that the requestor is who he purports to be? Is this individual allowed to read or modify the requested data? A SWS-Policy document defines what authentication tokens are acceptable as proof of identity for login. Upon initial access (arrow 1), a user is redirected to the Semantic Web authentication service (2) to establish identity and generate a biometric authentication token (3); this token is stored on the access device as a cookie (4), signed with the digital signature of the Secure Token Service (STS). Biometric authentication tokens are presented automatically upon subsequent logins. Each of this token is valid for a limited time; token expiration forces a revalidation upon subsequent login. Semantic Web portal applications, as opposed to humans, attempting to access data use digital signatures to authenticate their origin. After successful login, all Semantic Web portal data requests are sent to the organization's data repository and Semantic Web service (5) along with the user's biometric authentication token.

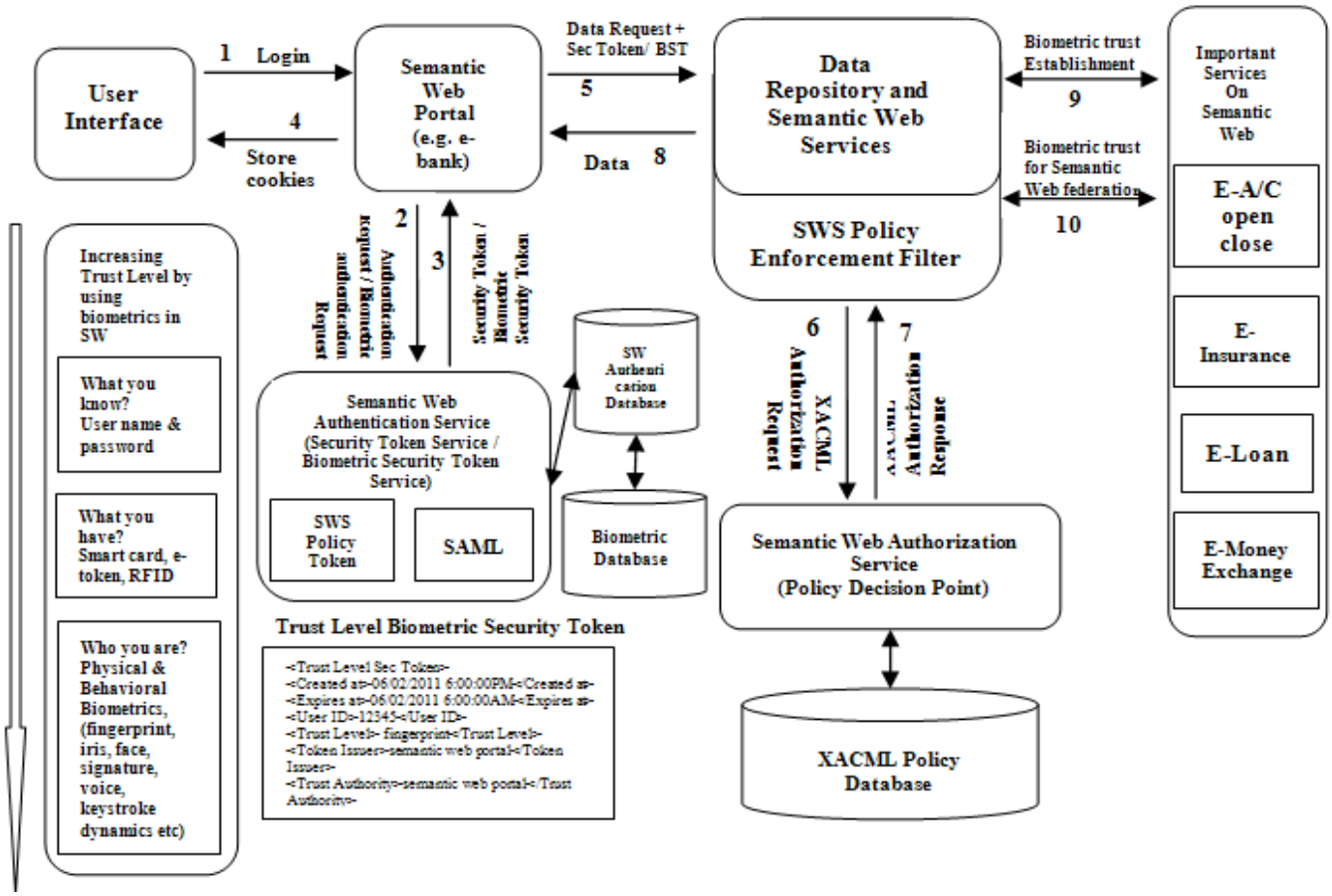

Figure 5. The increase in depth of trust than other authenticators (password, e-tokens) by using biometrics infrastructure for Semantic Web and its applications

The Semantic Web portal's SWS-Policy document will define the allowable or required biometric authentication tokens to be included with all data requests, while the organization's Semantic Web data repository service's SWS-Policy document will define both the biometric authentication and biometric authorization requirements for data access. All SWS-Policy documents should be XML-based. An example of Authentication Algorithms (Biometrics based Security Token Request and Reply) using XML is shown below.

Authentication (biometrics based security token) Token Request

```
<Authentication Token>
<Created At>06/03/2011 8:00:00 AM</Created At>
<Expires At>06/03/2011 5:00:00 PM</Expires At>
<Username>12345</Username>
<KeyStr>FINGERPRINT_KEY_STRING</KeyStr>
<Technology>Fingerprint</Technology>
</Authentication Token>
```

*Authentication (*biometrics based security token*) Token Reply*

```
<TrustLevelSecToken>
<Created At>06/03/2011 8:00:00AM</Created At>
<Expires At>06/03/2011 5:00:00 PM</Expires At>
 <UserID>12345</UserID>
<Trust Level>Fingerprint</Trust Level>
<TokenIssuer>semantic web portal address </Token Issuer>
<TrustAuthority> semantic web portal address </TrustAuthority>
</TrustLevelSecToken>
```

If the data repository service's SWS-Policy is simple, it can be enforced automatically using Semantic Web Service Enhancements; if the policies are complex, then SWSE can call predefine custom Semantic Web authorization service that will support custom policy assertions. In this case, the authorization engine will consult its XML-based authorization rule database to determine what permissions should be given to a particular user when attempting to touch a protected object. The biometric authorization engine will return an "access permitted" or "access denied" semantic notification decision based upon the user's identity, the user's role, the object being accessed, and the local context surrounding the access. In response to an authorized asynchronous event such as data access, semantic notification service can respond in multiple ways. Data could be displayed on the semantic web data portal, delivered to the legitimate user's access device. Semantic notification will tell about uploading, downloading, manipulation of data.

VII. EVALUATION OF THE MERITS OF THE PROPOSED FRAMEWORK

Evaluation of Technology

The advantages of proposed framework over traditional authentication methods, such as passwords, Smart Card [14] and RFIDs are well known. Hence, biometric systems are gradually gaining ground in terms of usage. Biometric systems identify users based on two traits i.e. physiological and behavioral characteristics [21]. According to website (www.techcast.org,) biometrics is expected to enter the mainstream (at a 30% adoption level) in 2015 with a $380 billion U.S. market size, a $1368 billion world market, predicted at a 73% expert confidence level [18]. It is obvious that no single biometric is the "ultimate" recognition tool and the choice depends on the application. A brief comparison of the biometric techniques

based on seven factors described below is provided in Table I [15]. Comparison of various biometric technologies based on the perception of the authors. High, medium, and low are denoted by H, M, and L, respectively. Universality (do all people have it?), distinctiveness (can people be distinguished based on an identifier?), permanence (how permanent are the identifiers?), and collectable (how well can the identifiers be captured and quantified?) are properties of biometric identifiers. Performance (matching speed and accuracy), acceptability (willingness of people to accept), and circumvention (foolproof) are attributes of biometric systems [17].

Table I.

Comparison of various biometric technologies based on the perception of the authors High, Medium, and Low are denoted by H, M, and L, respectively [15]

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

We compare various authenticators (password, token, and biometrics) with respect to security issues of Semantic web. Table II lists a number of potential attacks against user authentication with examples and typical defenses. Table III does the same for non-attack security issues. This evaluates the use of biometrics over the Semantic Web is more secure and better than other authenticators (password and e-token). If an authenticator is inconvenient, it will not be used, or will not be used properly, which may present vulnerabilities. Users who must remember multiple, changing passwords are notorious for abusing password rules. Though a token reduces the problem of remembering passwords, the user must remember to carry the physical object, which is sometimes inconvenient. Biometrics alleviates the problem of remembering anything, but some users experience inconvenience by false no match results. For tokens and biometrics in a networked application, there is an additional convenience issue of how to best register/enroll, renew, recover, and revoke the authenticator. Since a token is an object, it must be put into the hands of the authorized person either personally or by delivery. Correspondingly, it may need to be removed from the user if authorization is revoked.

Evaluations of Attacks and Security Issues

Table II. Evaluations of Attacks using different authenticators for Semantic Web

Attacks	Authenticators	Examples (Attack Types)	Defend against attacks
Client Attack	Password	Guessing, Exhaustive Search	Large entropy , limited attempts
	Token	Exhaustive Search	Large entropy , limited attempts
	Biometrics	False Match	Large entropy , limited attempts, theft of object requires presence
Server Attack	Password	Exhaustive Search, Dictionary search, Plain Text Theft	Hashing, large entropy, protection of password database (by administrator password or encryption)
	Token	Pass-code Theft	One time pass-code per session
	Biometrics	Template Theft	Capture device authentication
Eavesdropping, Piracy, Theft, Copying	Password	Shoulder Surfing	User diligence to keep secret, administrator diligence to revoke compromised passwords, multi factor authentication
	Token	Theft	multi factor authentication, temper resistance, evident hardware token
	Biometrics	Spoofing (Copying) biometric	Copy detection at capture device and capture device authentication

Denial of Service Attack	Password, Token, Biometrics	Lockout by multiple failed authentication	Multi factor with token
Replay Attack	Password	Replay Stolen Password Response	Challenge response protocol
	Token	Replay Stolen Pass-code Response	Challenge response protocol, One time pass-code per session
	Biometrics	Replay Stolen Biometric template Response	Copy detection at capture device and Capture device authentication via Challenge response protocol,
Malware Attacks (Virus, Worm, Trojan Horse)	Password, Token, Biometrics	Installation of infected device or rouge client	Authentication of client or capture device, capture device or client with a trusted security perimeter

Table III. Evaluations of Security Issues using different authenticators for Semantic Web

Security Issues	Authenticators	Examples	Defend against attacks
Non-repudiation	Password/ Token	Claim lost or stolen password	Personal liability
	Biometrics	Claim copied biometric	Copy detection at capture device and Capture device authentication
Compromise detection	Password/ biometrics	Stolen password or copied biometric	Last login displayed to user to detect anomaly
	Token	Lost or stolen token	User notes physical absence
Administrative and policy registration enrollment	Password	Initial password registration	Delivery to pre established email address
	Token	New token registration	Delivery to pre established postal address
	Biometrics	Biometric enrollment	In person with picture identity
Administrative and policy reset and recovery	Password	Forgotten password	Secondary authenticator (e.g. date of birth)
	Token	Lost token	Delivery to pre established postal address
	Biometrics	Compromised Biometric	Not much options but revert to password

Evaluation of Cost

The cost is associated with the depth of security needed. The tolerable cost of an authentication system is dependent upon the application of Semantic Web. One way to quantify this is to estimate the cost of the minimum-security implementation that makes the cost of attack to the attacker more than his maximum potential gain. However, this gambles that the attacker is fiscally rational. It is better to estimate the cost of loss to the attacked party and implement security to reduce the risk of successful attack to a chosen low probability.

There are three types of cost. One is the per-user cost. A password scheme costs nothing per user (if the user has a keyboard or keypad), whereas a biometric recognition [16] requires a reader at the client, and a token requires a reader and the token itself. Infrastructure costs can be large but are usually reduced on a per-client basis if that number is high. This is in contrast to the third cost, administration. Administrative costs (for example, for reset when a password is forgotten or token is lost) may be the most important consideration. The following section concludes the result as consequences of proposed framework for semantic web security.

VIII. CONSEQUENCES OF FRAMWORK

We believe that a biometrics security approach represents a promising technology for protecting data on Semantic Web in the organizations. Enhanced security is thought to be the greatest benefit of biometric technologies, followed by accuracy. Other benefits are its unique feature of not being shared/copied/lost, it reduces paperwork, and it is convenient [18]. It is also shown in figure 6 below. To that end we have to build an operational prototype with these working components:

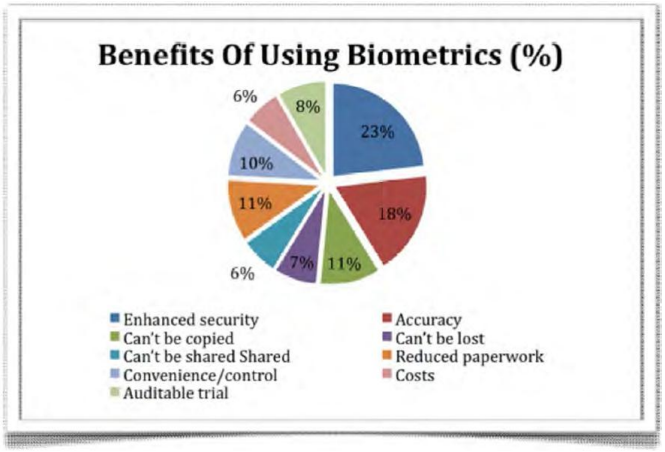

Figure 6. Benefits of using biometrics [18]

Semantic Web Portal

SW portal is the common entry point for human access to Semantic data and data repositories. Our technological mission is to create a secure and satisfying ontology management environment needed for Semantic Web enabled community portals and to make extensive usage of Semantic Web technologies for enhanced information processing facilities and to create secure means for the Semantic inter-operation between different communities and even different Semantic Web portals [19].

Biometric Authentication

We should have to use a common approach to all identification mechanisms so that authorization can keep pace with the rapid change of technology. Authentication module will generate authentication tokens for all types of authenticators (passwords, fingerprints, iris scans, signature recognition, e- Tokens and key fobs (random number generators).

Biometric Authentication Trust Levels

It is well known that different authenticators have different levels of reliability. We have introduced the concept of biometric trust level, a numerical representation of the reliability underlying each identification technology. Biometric trust levels will be established scientifically by determining a technology's false acceptance and false rejection rates. Biometric trust levels can then be used as a component of an authorization rule for Semantic Web Security Policy.

On-demand Authentication

Legitimate Users may prove their identity using any authenticator available on their access device for Semantic Web Portal. Usage will proceed until the legitimate user will attempt to access an object whose access rule requires a higher trust level of authentication than currently provided by the user's authentication token. At that point the legitimate user is given the opportunity to upgrade higher authentication token using a technology of higher reliability.

Token Substitution

A higher reliable authenticator can substitute low reliable authenticator. A biometric authorization rule may permit a higher-reliability biometric authentication token to substitute for the lower-reliability authentication token that would normally be required, without requiring a secondary sign-on and authentication procedure.

Biometric Authorization

Administrators, Organizers or policy makers may define an access rule to protect any object in the Semantic Web. Rules will be evaluated dynamically (e.g. upon each access) and will be context-aware. Rules may be arbitrarily complex and will be evaluated using a combination of system-provided primitives, local functions, and custom Semantic Web services designed by the legitimate user. An access rule can be a reference time, location, identity, roles, local conditions, and current circumstances, such as: "Access to data D is granted to user U with identity I if U is an employee of company C and either (a) the access request can come from a wired device within the organization and the legitimate user has authenticated at a best level of authenticator, or (b) the access request can come from a wireless device and the legitimate user has authenticated at a biometric trust level of fingerprint or higher."

Policy-driven Semantic Web Security

All types of authentication, authorization including biometric authentication and biometric authorization, and trust federation rules can be expressed in XML, SAML etc in SWS-Policy documents.

Biometric Trust for Semantic Web Federation

Biometric Federated Systems can operate across organizational and technical boundaries, including different operating systems and different security platforms. Any organization is one component of a modem infrastructure of corporate, education, tourism etc like e-banking and e-learning, e-tourism. Auxiliary services such as e-money exchange, e-loan, and e-insurance and alternative websites, e-education are likewise important players (see figure 5). We can use trust authorities, trust groups, and trust mapping to reliably manage and exchange authenticator (user credentials/password, e-tokens, biometrics) among trust domains.

Devices

We can process access requests from various devices ranging from wired to wireless for e.g. PCs, laptops, Pocket PCs and Tablet PCs, mobile [20]. Biometric Authorization rules may require higher reliable authenticator from wireless devices for more stringent security standard purpose as wireless protocol suites has more vulnerabilities than wired one.

Semantic Notification

In response to an authorized asynchronous event such as data access, semantic notification service can respond in multiple ways. Data could be displayed on the semantic web data portal, delivered to the legitimate user's access device. Semantic notification will tell about uploading, downloading, manipulation of data.

IX. CONCLUSIONS & FUTURE WORK

In this paper, we approach towards Defending against Attacks by Enhancing Security using Biometrics in Semantic Web. Biometrics generated templates and token is efficient mutual authentication mechanism. Using biometrics in consideration of the restrictive characteristic of Semantic Web it is designed in secure framework. Moreover security problem of client and service provider was solved by using the biometrics infrastructure. Security tokens are used for the availability inspection of a legitimate user at best use. At the same time, mobile users need efficient biometric enabled system in distributed form for minimizing the overload of authentication. Biometrics play critical role to secure data transmission and privacy of clients as well as Semantic Web service providers. For interoperability of Semantic Web services and applications, which use biometrics, must be cross verified. Secure interoperability between both and all database system need to find out the best solution for next generation of WWW security. Security and interoperability (Secure Interoperability) are burning challenges of today's internet technologies. Semantic Web needs in future to conduct research on intrusion detection, malicious attack prevention as well as critical infrastructure protection for the Semantic Web service oriented architecture. It means Semantic Web has to survive in unauthorized, malicious attacks and system failures region. So biometrics can be next substitute to make secure interoperable communication in distributed computing systems. All templates of biometrics system assumed to encrypt or decrypt xml credential before transmission into unsecured channel. Finally, our future work will focus on finding more use cases and real world scenarios to validate the efficiency of our approach and determine the feasibility of the Semantic match of lightweight ontologies and mappings in particular contexts of biometrics.

REFERENCES

[1] Thuraisingham B., Parikh P., "Trustworthy Semantic Web Technologies for Secure Knowledge Management", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing 2008 (EUC '08), Issue Date: 17-20 Dec. 2008,

[2] World Wide Web Consortium, www.w3.org

[3] Fensel, Dieter Andreas, "Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce" Springer-Verlag, 2002.

[4] O'Gorman L., "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proceedings of the IEEE, Volume.91 no.12, 2003, pp. 2021 – 2040

[5] B. Lee, J. Hendler and Ora Lassila,"The Semantic Web", Scientific American Magazine", May 17, 2001.

[6] B. Thuraisingham,"Building Secure Survivable Semantic Webs", 14th IEEE International Conference on Tools with Artificial Intelligence, 'ICTAI'-2002.

[7] Bhavani Thuraisingham, "Confidentiality, Privacy and Trust Policy Enforcement for the Semantic Web", 8th IEEE International Workshop on- Policy for Distributed System and Network, 2007.

[8] Fugkeaw S., Manpanpanich, P., Juntapremjitt, S., "A Robust Single Sign-On Model Based on Multi-Agent System and PKI", IEEE Sixth International Conference on Networking, 2007, ICN '07, 22-28 April 2007, pp. 101 – 101.

[9] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models",IEEE Computer, vol. 29, no. 2,Feb. 1996,pp. 38-47.

[10] David Geer, "Taking Steps to Secure Web Services", Computer,IEEE Technology News, Oct 2003

[11] Bhavani Thuraisingham, "Confidentiality, Privacy and Trust Policy Enforcement for the Semantic Web", POLICY '07 Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks, 2007.

[12] Bhavani Thuraisingham,"Security Issues for the Semantic Web", Proceedings of the 27th Annual International Computer Software and Applications Conference, COMPSAC-03, IEEE Computer Society,2003,pp.632

[13] Ratha, N. K.; Connell, J. H.; Bolle, R. M.; "Enhancing security and privacy in biometrics-based authentication systems" IBM Research Division, IBM Systems Journal, 2001, Volume: 40,no.3, pp. 614 – 634.

[14] Riza Cenk Erdur , Geylani Kardas," Personalized Access to Semantic Web Agents Using Smart Cards", *Euro-Par 2005*, Lecture Notes in Computer Science, 2005, Volume 3648/2005, 621,pp. 1110-1119, DOI: 10.1007/11549468_121

[15] Jain, A.K., Ross, A., Prabhakar, S., "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, January 2004,Vol. 14, No. 1, pp 4-20

[16] Prabhakar S., Pankanti S., Jain A.K., "Biometric Recognition: Security and Privacy Concerns," Security & Privacy IEEE, Mar-Apr 2003, Vol. 1, No. 2, pp. 33–42

[17] C. Soutar, Biometric System Security White Paper, Bioscrypt [Online]. Available: http://www.bioscrypt.com

[18] Vivian Chu and Gayathri Rajendran, "USE OF BIOMETRICS", TechCast Article Series, the George Washington University, TechCast LLC, 2009.

[19] Semantic Web Portal Project, http://sw-portal.deri.at/

[20] Matthias Wagner, Massimo Paolucci, "Enabling Personal Mobile Applications through Semantic Web Services", DoCoMo Communications Laboratories Europe,*www.w3.org/2005/04/FSWS/Submissions/.../DoCoMo-Pos-Paper.pdf*

[21] Jain, A.K., Ross, A., Pankanti S., "Biometrics: A Tool for Information Security", IEEE transactions on information forensics and security, vol. 1, no. 2, 2006, pp. 1556-6013.

[22] Kumar, S. Prajapati, R.K. Singh, M. De, A., "Security Enforcement using PKI in Semantic Web", International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010 ,pp. 392 – 397., Digital Object Identifier: 10.1109/CISIM.2010.5643507

[23] Hendler, James, Berners-Lee, Tim and Miller, Eric "Integrating Applications on the Semantic Web," Journal of the Institute of Electrical Engineers of Japan, Volume 122(10), October, 2002, p. 676-680.

[24] H. Peter Alesso, Craig F. Smith, "Thinking on the Web: Berners-Lee, Gödel and Turing", second edition, John Wiley & Sons, Inc., 2010, pp. 177-189., ISBN: 978-81-265-2414-3

[25] Lu Liu, Deyu Kong, Yi Li and Zhe Liu, "An Approach to Enterprise Application Integration Based on Ontology Semantic Description", Research and Practical Issues of Enterprise Information Systems II, IFIP International Federation for Information Processing, 2008, Volume 255/2008, 977-982, DOI: 10.1007/978-0-387-76312-5_21

[26] Alexander Felfernig, Gerhard Friedrich, Dietmar Jannach, Markus Stumptner and Markus Zanker, "Acquiring Configuration Knowledge Bases in the Semantic Web Using UML", Knowledge Engineering and Knowledge Management: Ontologies and the Semantic Web, Lecture Notes in Computer Science, 2002, Volume 2473/2002, pp. 141-151, DOI: 10.1007/3-540-45810-7_31

[27] Arash Shaban-Nejad, Christopher J. O. Baker, Volker Haarslev and Greg Butler, "The Fungal Web Ontology: Semantic Web Challenges in Bioinformatics and Genomics", The Semantic Web – ISWC 2005, Lecture Notes in Computer Science, Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2005, Volume 3729, pp.1063-1066, DOI: 10.1007/11574620_78

[28] Maedche A., Motik B., Stojanovic L., Studer R., Volz R., "Ontologies for enterprise knowledge management", Intelligent Systems, IEEE, 2003, Volume: 18 Issue:2, pp. 26 – 33, DOI: 10.1109/MIS.2003.1193654

[29] Oscar Corcho, Silvestre Losada, Richard Benjamins, José Luis Bas and Sergio Bellido, "Personal eBanking Solutions based on Semantic Web Services", E-Service Intelligence, Studies in Computational Intelligence, 2007, Volume 37,pp. 287-305, DOI: 10.1007/978-3-540-37017-8_13

[30] Wenya Tian and Yuxin Mao, "A Semantic Grid Application for E-Learning Data Sharing", Advances in Web Based Learning - ICWL 2008, Lecture Notes in Computer Science, 2008, Volume 5145/2008, 457-467, DOI: 10.1007/978-3-540-85033-5_45

[31] Hepp, Martin, "GoodRelations: An Ontology for Describing Products and Services Offers on the Web", Proceedings of the 16th International Conference on Knowledge Engineering and Knowledge Management (EKAW2008), Acitrezza, Italy, September 29 - October 3, 2008, Springer LNCS, Volume 5268, pp. 332-347.

[32] RSA, "Securing Your Future with Two-Factor Authentication", http://www.rsa.com/node.aspx?id=1156 (viewed on 20 April 2011)

[33] Massimo Paolucci, Takahiro Kawamura, Terry R. Payne and Katia Sycara, "Importing the Semantic Web in UDDI", Web Services, E-Business, and the Semantic Web, Lecture Notes in Computer Science, 2002, Volume 2512/2002, 815-821, DOI: 10.1007/3-540-36189-8_18

Short biodata of all the author

Akhilesh Dwivedi received the B.Tech degree in Electronics and Telecommunication Engineering from the MGM College of Engineering & Technology, Noida (U.P. Technical Univ., Lucknow) India, in 2009 and pursuing M.Tech in Information Security from Ambedkar Institute of Technology, Govt. of NCT Delhi, Geeta Colony, New Delhi (Guru Govind Singh Indraprastha University, New Delhi), India.

His main research interests are in Cryptography and Network Security, Biometric Security and Secure Semantic Web Services, Data Storage Security in Cloud Computing. Mr. Dwivedi is the life-time member of AIRCC, IAENG, IACSIT, and IAOE. He is the author/co-author of more than 7 publications in International/National journals and conferences.

Suresh Kumar received the M.Tech degree in Computer Science & Engineering from Department of Computer Science & Application, Kurukshetra University, Kurukshetra, Haryana, India in 2002 and pursuing Ph.D. from Faculty of Engineering & Technology, Maharshi Dayanand University, Rohtak, Haryana, India. His major field of study is Semantic Web. His current research interest includes Secure Semantic Web Services, Semantic Search, Cloud Computing, Cryptography and Network Security, Biometric Security.

He has more than nine years teaching experience. He is working as Assistant Professor in the Department of Computer Science & Engineering, Ambedkar Institute of Technology, Govt. of NCT Delhi, Geeta Colony, New Delhi, India. He is the author/co-author of more than 13 publications in International/National journals and conferences.