Cancellable Biometrics for Security and Privacy Enforcement on Semantic Web

Akhilesh Dwivedi
Department of CSE,
AIT, New Delhi, India

Suresh Kumar
Department of CSE,
AIT, New Delhi, India

Abhishek Dwivedi
Department of MCA,
RKGEC, Ghaziabad, India

Manjeet Singh
Department of CE,
YMCA UST, Faridabad India

ABSTRACT
The entire vision of the Semantic web has nonetheless to be totally accomplished, however there has been considerable progress inside the development and use of standards, languages, technologies and applications. Hence, the Semantic web must be conscious of different types of risks, privacy issues and security issues to stay efficient and secure. Biometric systems provide the answer to confirm that only a legitimate user and nobody else access the rendered services. The safety depends on the secrecy, privacy and trustworthiness of the authenticators because deeper the trust level of authenticator, stronger are going to be security and privacy of Semantic web. Cancellable biometrics and secure sketches have been introduced with the same purpose to guard the privacy of biometric templates to enhance the security and privacy of Semantic Web Services.

General Terms
Cancellable biometrics, Security, Privacy, Semantic Web

Keywords
Biometrics, BioHash, Security, Privacy, Semantic Web, Trust

1. INTRODUCTION
The Semantic Web provides a powerful, standardized, worldwide, ubiquitous communications mechanism whose benefits are impossible to ignore [1]. We think that Internet accessible information is the clear wave of the future, if 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. As promoted by the World Wide Web Consortium (W3C) [2] Semantic Web Service interactions permits planning, designing, publishing, promoting, registering, and initiating processes dynamically in an exceedingly distributed computing surroundings. 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]. 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 concentrated 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]. 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. A number of biometric characteristics are in use in numerous applications [6] (see Fig. 1). Each biometric has its strengths and weaknesses, and the selection depends on the application. The benefit of adding biometrics in Semantic Web is to provide empowerment and more security and privacy to Semantic Web. In this paper, we present our approach for protecting against attacks and enhancing security as well as privacy using biometrics in Semantic Web.

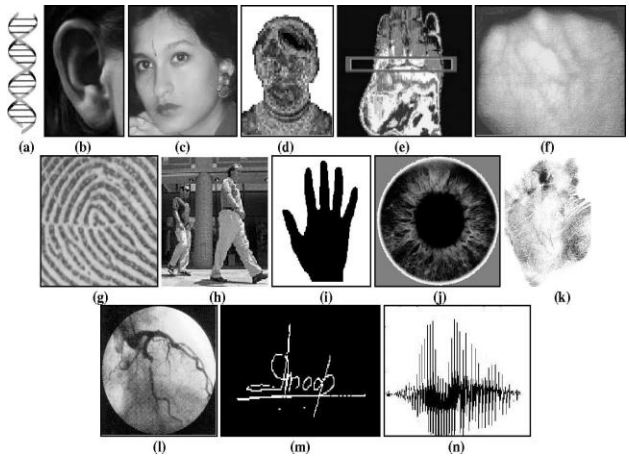

Fig 1: Examples of biometric characteristics: (a) DNA, (b) ear, (c) face, (d) facial thermo gram, (e) hand thermo gram, (f) hand vein, (g) fingerprint, (h) gait,(i) hand geometry, (j) iris, (k) palm print, (l) retina, (m) signature, and (n) voice [6]

2. SECURITY AND PRIVACY ISSUES OF SEMANTIC WEB
Key applications of semantic web [7,8] are e-banking [13], e-learning [14], e-commerce [15], Semantic Search [8], Bioinformatics [11], Knowledge Management [12], Semantic based Enterprise application and data integration [9], Knowledge Base [10] etc. These areas of application require a high level of security and privacy. Therefore, we need to focus on 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 and privacy. Nevertheless, it would clearly not be feasible to remember the user authentication based on so much big key every time. So Biometrics may be introduced to provide security and privacy to the Semantic web. 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 [16]. The biometric approach suffers from the privacy invasion and no revocable problems. Passwords and tokens are simply forgotten and lost. To address these problems, the notion of cancellable biometrics was introduced to denote biometric templates, which will be cancelled and replaced with the inclusion of another freelance authentication issue. BioHash may be a type of cancellable biometrics, which mixes a group of user-specific random vectors with biometric features. BioHash is in a position to deliver extraordinarily low error rates as compared to the only real biometric approach when a real token is employed. However, this raises the likelihood of two identity theft scenarios: (i) stolen-biometrics, within which an impostor possesses intercepted biometric data of sufficient prime quality to be thought of real and (ii) stolen-token, within which an impostor has access the real token and the impostor to claim as the legitimate user utilizes it [27]. This paper proposes a user-centric approach to increase the depth of trust of Semantic Web security and privacy. Here cancellable biometric approach is used to deal with the privacy issue.

The next section elaborates based on following terms and proposes our novel idea in this regard.

- Security enforcement using biometrics in semantic web
- Privacy enforcement using biometrics in semantic web

3. SECURITY ENFORCEMENT USING BIOMETRICS IN SEMANTIC WEB

According to website (www.techcast.org,) biometrics is anticipated 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% professional confidence level [17, 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 in Table I [16]. Comparison of various biometric technologies based on the perception of the authors. H, M, and L denote high, medium, and low, 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 [16].

The key objectives of security enforcement using biometrics in Semantic Web [18],

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

As shown in fig.2 these key objectives are tried to achieve and are explained [18].

Table 1. Comparison of Various Biometric Technologies Based on the Perception of the Authors. H, M, and L, denote high, medium, and low respectively [16]

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

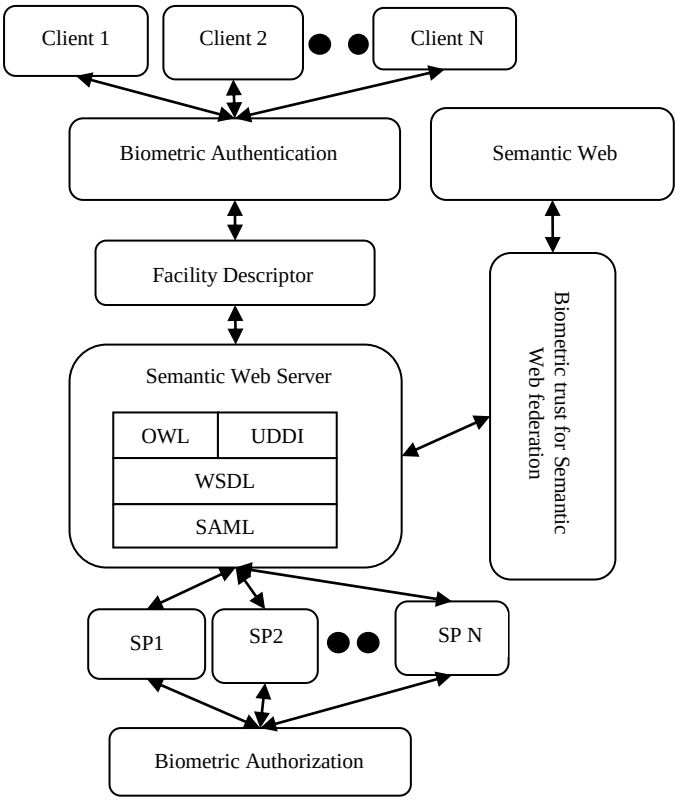

Fig 2: Security enforcement using biometrics in Semantic Web [18]

3.1 Client

Clients are entities, who are availing these published services from Web server. Some of them may be freely available other may chargeable. Client is a consumer of services running on Semantic Web server.

3.2 Biometric Authentication

It is vital to notice that biometrics-based authentication systems be designed to resist attacks when utilized in security-critical applications, particularly in unattended remote applications like e-commerce [19]. For biometrics ("who you are"), the enrolment of templates into authentication database of Semantic web. That works on the principal that who you are? Additionally, do support that you just are you. Varied sorts of scanners are out there for various kinds of functions of enrolment of templates in database. The RSA SecurID [20] system needs a password ("what you know") and the proper random number while login ("what you have").

3.3 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. 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" [21, 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.

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) [18]. 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 that are nevertheless successful; the false rejection rate is the percentage of authentication attempts by the enrolled individual, which are nevertheless rejected [6].

3.4 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 [23].

3.5 Semantic Web Server

Semantic Web Server is common, distributed platform to fetch and retrieve data by using Semantic Web services throughout internet.

3.5.1 OWL

Ontology Web language are use to describe ontology [18]. Ontology usually consists of a hierarchical description of vital ideas 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].

3.5.2 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. 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.

3.5.3 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 defines 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].

3.5.4 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 [24].

3.6 Service Providers

Service providers are organization's 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 [5].

3.7 Semantic Web Services

They are self-contained, self describing, modular applications which will be revealed, located, and invoked across the semantic web. "Once a Web service is deployed on server applications or other Web services can discover and invoke all those service" [25].

3.8 Biometric Authorization

In the conventional role-based access control (RBAC) model [26], 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 outlined as a restriction, which will be applied by the authorization policy: permission P is granted to role R with identity I if and on condition that constraint C is satisfied. Various sorts of contexts are attainable; however, we tend to are mainly involved with the context of the present access request (e.g., the status of the user creating a request; the status of the article being requested; when and where the request originated). By adding context-based constraints to the authorization policy, authorization will be determined dynamically primarily based upon the present context of the request, instead of simply the role of the user.

3.9 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 that including different operating systems and different security platforms. Biometric Federation will depend upon two authorities being resident in each domain [18].

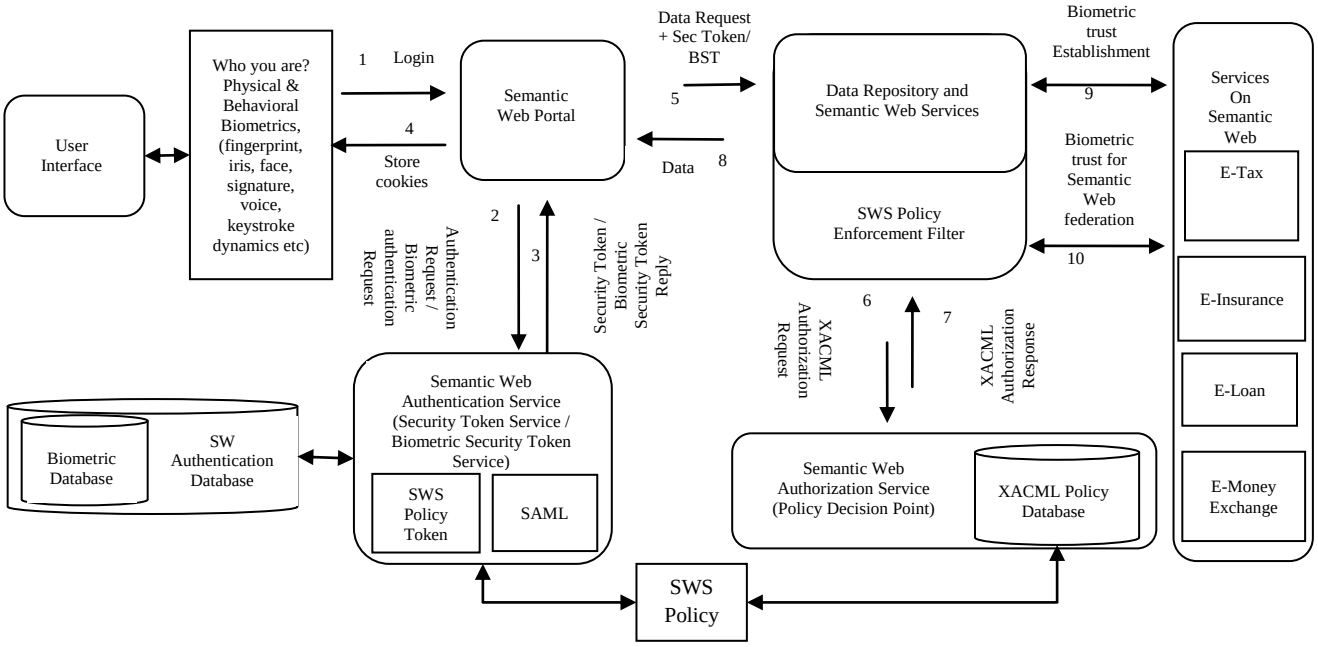

Fig 3: Biometric Security Infrastructure for Semantic Web and its applications

3.10 Biometric Security Infrastructure for Semantic Web

As illustrated in figure 3, 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 data Web service. 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 data Web service (5) along with the user's biometric authentication token [18].

4. PRIVACY ENFORCEMENT USING BIOMETRICS IN SEMANTIC WEB

Privacy has become an important issue in many aspects of our daily life. When sensitive data like biometrics is employed, the privacy problems become even additional vital because of corruption of such data could also be catastrophic for the relevant applications on Semantic Web.

4.1 BioHashing

As shown in fig.4 for authentication purposes, we can use simple hashing as well as hashing techniques using "biometric templates" that is called BioHashing techniques on Semantic Web. Passwords are typically stored in the database after they are hashed; when a new password is received, it is hashed and compared with the password hashed at enrollment. If a person has access to the database of hashed passwords, a password is not compromised. A similar analogy is applied to fingerprints. Solely one-way transformed illustration is stored and therefore, if an adversary has an access to the database, the biometric data is not compromised on Semantic web. BioHash combined the biometric template (face, fingerprint and palm print biometrics, which might be represented as a set length and ordered feature vector) with user-specific Tokenized Random Numbers (TRN) to provide a collection of noninvertible binary bit strings [27].

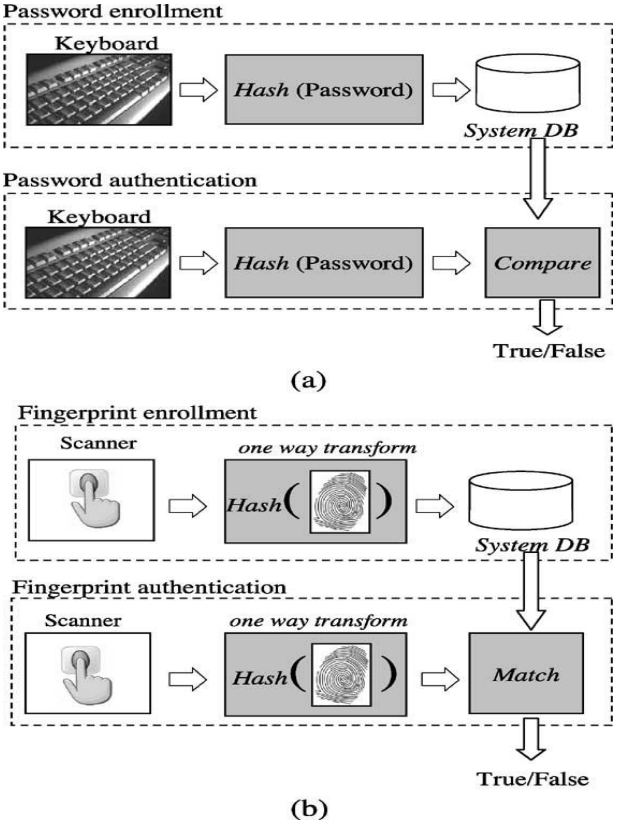

Fig 4: Biometric Authentication based on "private templates" using hashing techniques. (a) Passwords are typically stored in the database after they are hashed; when a new password is received, it is hashed and compared with the password hashed at enrollment. If a person has access to the database of hashed passwords, a password is not compromised. In (b), a similar analogy is applied to fingerprints. Only one-way transformed representation is stored and thus, if an adversary has an access to the database, the biometric information is not compromised [16].

The BioHash relies on each, biometric and TRN and it is irreproducible while not presenting the two simultaneously. BioHash is truly primarily based on the only use of TRN; thus, they conjectured that the introduction of any sorts of biometrics becomes meaningless since the system will solely have faith in the tokens without a flaw [28, 29]. We tend to address the two considerations of BioHash through its mathematical model. We show that BioHash is an ensemble of quantized random projections (RPs) that preserves the intra-class variations whereas enhancing the inter-class variations when the real token is employed}. On the other hand, the result reverts to the initial performance or slightly poorer within the stolen-token situation. Stolen biometrics situation, during which fraudulent verification is tried using solely intercepted biometric information related to the real user, however without the associated token [27].

The initial BioHashing [30] scheme is simplified and described as follows:

(i) Feature extraction is used to extract the biometric feature from the raw input. The biometric feature is represented as a fixed-length vector, $\Gamma \in R^n$ with n being the length of Γ.

(ii) Random basis generation using a user-specific TRN to generate **m**orthonormal pseudo-random vectors, $\{\mathbf{r}_{\perp \mathbf{i}} \in \mathbf{r_n} | \mathbf{i} = \mathbf{1}, \ldots, \mathbf{m}\}$ and $\mathbf{m} \leq \mathbf{n}$

(iii) Token and biometric mixing via $\{< \boldsymbol{\Gamma} | \mathbf{r}_{\perp \mathbf{i}} > | \mathbf{i} = \mathbf{1}, \ldots, \mathbf{m}\}$ with $\langle . \mid . \rangle$ indicating the inner product operation.

(iv) Binary discretisation to compute an m bit BioHash template, $\mathbf{b} = \{\mathbf{b_i} | \mathbf{i} = \mathbf{1}, \ldots, \mathbf{m}\}$ from $\mathbf{b_i} = \begin{cases} \mathbf{0} & \mathbf{if} \quad \langle \boldsymbol{\Gamma} \parallel \mathbf{r}_{\perp \mathbf{i}} \rangle \leq \boldsymbol{\tau}, \\ \mathbf{1} & \mathbf{if} \quad \langle \boldsymbol{\Gamma} \parallel \mathbf{r}_{\perp \mathbf{i}} \rangle > \boldsymbol{\tau}, \end{cases}$ with $\boldsymbol{\tau}$ being an empirically determined threshold.

4.2 Cancellable Biometrics

Cancellable biometrics can be a good option for privacy enforcement in Semantic Web and its applications because it provides higher privacy to the multiple templates associated with the same biometric data. The concept of cancellable biometrics was introduced [31, 32] to denote biometric templates that can be cancelled and replaced, as well as being unique for every application. Cancellable biometrics requires storage of the transformed (not actual) version of the biometric template and hence provides higher privacy levels by allowing multiple templates to be associated with the same biometric data.

There are three principal criteria to be fulfilled before a cancellable biometric template can be considered useful [27, 33]:

(i) Diversity: no same cancellable template can be used in two different applications.

(ii) Reusability: straightforward revocation and reissuance in the event of compromise.

(iii) One-way transformation: non-invertibility of template computation to forestall recovery of secret biometric data.

These methods generally fall into three categories:

- Error correcting based
- Integration of external factors and biometrics
- Noninvertible transforms.

4.2.1 Error-Correcting Code

In this scheme, codeword and decoding functions are established from the biometric templates during enrolment. The codeword value can be used either as a key or as hash. At the authentication stage, the input biometric data are used to compute or recover the codeword.

4.2.2 Integration of External factors and Biometrics

Soutar et al. [34] first proposed the second approach of integrating an independent factor with biometric features. They described a different approach for generating cancellable biometrics from fingerprints using optical computing techniques. With a few fingerprint images and a set of random numbers for training, the algorithm creates a complex-valued correlation filter function, which is mathematically optimized to possess both distortion tolerance and discrimination properties. In Table 2, we provide a comparison of various algorithms: Soutar et al., Davida et al. Monrose et al., Linnartz and Tuyls, Juels and Sudan, and Clancy et al. The third column in Table 2 indicates the key release (R) or key generation (G) classification. Practicality deals with the complexity of the algorithm. The sensitivity of a scheme was assessed based on our perception of whether the algorithm can tolerate realistic variations in the biometric signal such as noise, variable length representation, unordered representation, unaligned representation, etc. In the last four columns H, M, and L denote high, medium and low, respectively. Rigorous security analysis for the first two algorithms has not been provided (U) [16].

Table 2. Comparison of varied Biometrics-Based Key Generation and Key release Algorithms primarily based on the perception of the Authors [16]

Algorithm	Biometric (representation)	Classification	Privacy protection	Practicality	Sensitivity to invariance	Security
Soutar et al.	Fingerprint (image)	R	H	M	H	U
Davida et al.	Iris (IrisCode)	G	H	H	L	U
Monrose et al.	Keystroke, Voice	G	H	H	H	M
Linnartz and Tuyls	No evaluation	G	H	L	L	H
Juels and Sudan	No evaluation	G	H	H	L	H
Clancy et al.	Fingerprint (minutiae)	G	H	H	M	H

4.2.3 Non-invertible Transforms

Non-invertible transformed-based approach, rather than storing the initial biometric; the biometric is remodeled employing a one-way function [27]. The transformation happens within the same signal or feature space because the original biometric. For example, Bolle et al. [32] introduced an intentional distortion of a biometrics signal based on a chosen transform function. The biometrics signal was distorted within the same fashion at every presentation, that is, throughout enrolment and for each subsequent authentication. With this approach, each instance of enrolment will use a special distinct transform function therefore rendering cross matching not possible.

5. SECURITY AND PRIVACY ANALYSIS

5.1 Analysis of Security Issues

We compare various authenticators (password, token, and biometrics) with respect to security issues of Semantic web. Table 3 describes it for security issues. This evaluates the use of biometrics over the Semantic Web is more secure and better than other authenticators (password and e-token).

Table 3. Analysis of Security Issues using different authenticators for Semantic Web [18]

Security Issues	Authenticators	Examples	Attacks' Protection
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 enrolment	Password	Initial password registration	Delivery to pre-established email address
	Token	New token registration	Delivery to pre-established postal address
	Biometrics	Biometric enrolment	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

5.2 Analysis of Privacy Issues

The privacy of Semantic Web relies on privacy of biometric hashes. In this section, we tend to prove the non-invertible property of Bio-Hash, in order that it is computationally tough to recover the biometric feature from the BioHashes. This property ensures that solely the mixture of TRN and biometrics feature will contribute to the authentication method on Semantic web. We tend to additionally take into account attainable ways in which the BioHash could also be attacked and discuss how the new BioHash construction circumvents these attacks the protection analysis of non-invertible property will by considering earlier description of the RP, $\boldsymbol{v = R\Gamma}$ where R is an $\mathbf{m} \times \mathbf{n}$ orthonormal random matrix and $\mathbf{m} < \mathbf{n}$. The vector v will be considered a collection of underdetermined systems of

linear equations (more unknowns than equations). Therefore, it is not possible to seek out the precise values of all the elements $\boldsymbol{\Gamma}$ by solving an underdetermined linear equation system in $\boldsymbol{v} = \boldsymbol{R\Gamma}$ if $\mathbf{m} < \mathbf{n}$, based on the premise that the possible solutions are infinite. We adopt a formal proof that is described in Ref. [35] and [36]. Assuming both $\boldsymbol{R}$ and $\boldsymbol{\Gamma}$ are known, the system can be analyzed by the $\boldsymbol{QR}$ factorization of $\boldsymbol{R^T}$ such that $\boldsymbol{R^T} = \boldsymbol{Q}\begin{pmatrix}\bar{R}\\ \mathbf{0}\end{pmatrix}$

Where Q is an $\mathbf{n} \times \mathbf{n}$ orthogonal matrix and $\bar{\mathbf{R}}$ is an $\mathbf{m} \times \mathbf{m}$ upper triangular matrix.

If R is full rank, i.e. $\mathbf{rank}(\mathbf{R}) = \mathbf{m}$, there is a unique solution for $\boldsymbol{\Gamma}_{\mathbf{min\_norm}}$ that minimizes $\|\boldsymbol{\Gamma}\|_2$:

$$\boldsymbol{\Gamma}_{min\_norm} = \boldsymbol{Q}\begin{pmatrix}\bar{R}^{T^{-1}} & \boldsymbol{v}\\ \mathbf{0} & \end{pmatrix}$$

$$\boldsymbol{Q}\begin{pmatrix}\bar{R}\\ \mathbf{0}\end{pmatrix}(\boldsymbol{R^{-T}} \quad \bar{R})^{-1}\boldsymbol{v}$$

$$= \boldsymbol{Q}\begin{pmatrix}\bar{R}\\ \mathbf{0}\end{pmatrix}(\boldsymbol{R^{-T}} \quad \bar{R})$$

$$= \boldsymbol{R^T}(\boldsymbol{R} \quad \boldsymbol{R^T})^{-1}\boldsymbol{v}$$

$$= \boldsymbol{R^{\dagger}v}$$

Where $\boldsymbol{R^{\dagger}}$ is the pseudo-inverse of $\boldsymbol{R}$

$\boldsymbol{\Gamma}_{min\_norm}$ may serve as a starting point to the undetermined system, $\boldsymbol{v} = \boldsymbol{R\Gamma}$. The complete answer set will be characterized by adding an arbitrary vector from the null space of R, which might be created by the national basis for the null space of R, denoted by $\boldsymbol{\psi}$. It will be confirmed that $\boldsymbol{R\psi} = 0$ and which any vector v, where $\boldsymbol{\Gamma} = \boldsymbol{\Gamma}_{min\_norm} + \boldsymbol{\psi}_v$ for an arbitrary vector v satisfies, $\boldsymbol{v} = \boldsymbol{R\Gamma}$.

This result proves that even though the random matrix, $\boldsymbol{R}$ is understood to the adversary, it is not possible to seek out the precise values of all the elements in vector $\boldsymbol{\Gamma}$ of each undetermined system of linear equations utilized in Semantic web. Hence, Privacy of biometric templates defines the privacy of Semantic Web.

6. CONCLUSIONS

In this paper, we tend to approach towards security and privacy enforcement using Biometrics in Semantic web. Biometrics generated templates and token is efficient for mutual authentication mechanism. Using biometrics in thought of the restrictive characteristic of Semantic web, it has designed in secure framework. Moreover, security and privacy downside of client and service provider was solved by using the biometrics infrastructure. Security tokens are used for the provision inspection of a legitimate user at best use. At identical time, cancellable biometric allows privacy of semantic web highly. Biometrics play vital role to secure information transmission and privacy of clients additionally as semantic web and service providers. For interoperability of semantic web services and applications, that use biometrics, should be cross verify. Secure interoperability between each and every one database system have to be compelled to resolve, verify the most effective answer for next generation of WWW security. Security and interoperability (Secure Interoperability) are burning challenges of today's Semantic web technologies. We demonstrate the use of multi-state BioHash to resolve the stolen token problem in semantic web applications. BioHash could function as an effective cancellable biometrics to protect the privacy of the biometrics without compromising the recognition performance in the event of compromised token over Semantic Web. The BioHash is hence a substantive improvement over recognition based purely on biometric feature extraction and complex classifier for Semantic Web Services. Semantic web wants in future to conduct analysis on intrusion detection, malicious attack prevention additionally as vital infrastructure protection for the Semantic web service oriented design.

It suggests that Semantic web has to survive in unauthorized, malicious attacks and system failures region. Therefore, biometrics will be next substitute to create 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 concentrate on finding additional use cases and real world eventualities to validate the potency of our approach and confirm the feasibility of the semantic match of lightweight ontologies and mappings specifically contexts of biometrics.

7. 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. Handler and Ora Lassila, "The Semantic Web", Scientific American Magazine", May 17, 2001.

[6] 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

[7] Handler, 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.

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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.

[16] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil K. Jain, "Biometric Cryptosystems: Issues and Challenges", In Proceedings of IEEE, vol. 92, no. 6, June 2004, 948-960.

[17] Vivian Chu and Gayathri Rajendran, "Use of Biometrics", TechCast Article Series, the George Washington University, TechCast LLC, 2009

[18] Akhilesh Dwivedi et al "Defending Against Attacks By Enhancing Security Using Biometrics In Semantic Web", Journal of Global Research in Computer Science, Vol. 2, No 4,2011,pp.17-28.

[19] 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.

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

[21] 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.

[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] 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

[24] 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.

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

[26] 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.

[27] Andrew B.J. Teoha, Yip Wai Kuan, Sangyoun Lee, "Cancellable biometrics and annotations on BioHash", Pattern Recognition archive. Volume 41, Issue 6, June 2008, pp. 2034-2044, ISSN: 0031-3203.

[28] K.H. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, Revealing the secret of Face Hashing, ICB 2006, Lecture Notes on Computer Science,vol. 3832, Springer, Berlin. pp. 106–112.

[29] Kong, K.H. Cheung, D. Zhang, M. Kamel, J. You, "An analysis of BioHashing and its variants", Pattern Recognition 39 (7) (2005) 1359–1368.

[30] B.J. Andrew Teoh, C.L. David Ngo, A. Goh, BioHashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition 37 (11) (2004) 2245–2255

[31] N. Ratha, J. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (3) (2001) 614–634.

[32] R.M. Bolle, J.H. Connel, N.K. Ratha, Biometrics perils and patches, Pattern Recognition 35 (2002) 2727–2738.

[33] B.J. Andrew Teoh, A. Goh, C.L. David Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs", IEEE Trans. Pattern Anal. Mach. Intell. 28 (12) (2006) 1892–1901.

[34] C. Soutar, D. Roberge, A.R. Stoianov, Gilroy, B.V.K. Vijaya Kumar, Biometrics encryption, in: R.K. Nichols (Ed.), ICSA Guide to Cryptography, McGraw-Hill, New York, 1999, pp. 649–675.

[35] K. Liu, H. Kargupta, J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining", IEEE Trans. Knowl. Data Eng. 18 (1) 2006, pp. 92–106.