International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 6207-6216
© Research India Publications
http://www.ripublication.com

Service Oriented Secured Privacy Enhancement For Health Care Applications

Dr.S.Justin Samuel, Koundinya RVP, Kotha Sashidhar

Professor, Faculty of Computing,
Department of Information Technology, Sathyabama University, Chennai.
E.mail : drsjustin@gmail.com
UG Student, Faculty of Computing,
Department of Information Technology, Sathyabama University, Chennai.
E.mail : koundi.sathyabama@gmail.com
UG Student, Faculty of Computing,
Department of Information Technology, Sathyabama University, Chennai.
E.mail : kothasashidhar@gmail.com

Abstract

In online collaboration, privacy and trust factor among the developed web technology and distributed service are becoming more demand factors. Sometimes retrieving the data from the original source also finds its complex in the interconnected health care environment. In this paper, we introduce an e-Medical system for health care application with secret key generation and REST(REpresentational State Transfer). For the convenient and authenticated health care circle, privacy enhancement is enabled by generating the secret key mechanism. The trust factor is also increased with the implementation of REST. The secret is generated by the admin for the authentications; Once the communication is achieved the secret key will be automatically changed for the next client request. The blocking policy is also introduced to raise the trust factor and to prevent the medical details from scammers. By doing this, leakage of privacy polices get arrested. We propose a medical consultation and to open a secret account for HIV patients to communicate with hospital authorities by using privacy enhancement through online web services. The web service providers help the client with affordable web service policies.

Keywords: Service Privacy, e-Medical, REST, Service Policies

I INTRODUCTION

A web service plays a key role for various online applications by using UDDI, WSDL

Standards. Every application is characterized with a new generation of polices to satisfy the users needs. The ease of application extents its needs and qualities as E-medical service with composition of trust policies. The cause for the trust factor provides real time example in our day to day life. Verifying internships, bank balance, residential address, student's records, medical counseling are some of the web services provider in online business. Health care application becomes a significant online business using web services. However, the business develops trust factor gets decreased due to lack of authentication and security. This paper introduces a privacy enhancement to provide clients with various trust policies to enable authentication between the users and web service providers[1]. The online medical care also reduces the medical expenses and the quality of the medical service increased by introducing user preferable health care policies. The policies are provided for user stratification, each user can select their needs and it leads to select different optimal polices by generating secret key for each selection. Moreover, the patients' counts increases our system will act as a centralized service providers for each patients by fulfill their needs in convenient manner. E-Medical provides health care policies and virtual consultancy to the patients in convenient manner. This system is dynamic based treatment model with several unique policies. The service provider allows the clients to access the related information by verifying their authentication. The information from more than one source has been combined in data usage and the data are shared by common network in web based business. In the web service platform most of the data are shared among various clients, to maintain the security and privacy REST module is implemented with the composition of service polices[2]. Most of the application could not meet the user needs in dynamic environment and the active polices are not adorable for the users on the client side. So the newly improved computerized medical application is supportable for most of the health care services.

The main negative issues of computerized system are hacking, privacy, security. To ensure the privacy highly authenticated polices like finger print, security password, security questions, facial identifications, scan, etc., are provided. Data privacy and accuracy also increased by using efficient data retrieval techniques.

II RELATED STUDY

Salah-Eddine Tbahriti, Chirine Ghediraet et al[3] specify a privacy model that allows service to define set of privacy requirements in DaaS composition using UDDI and WSDL.WSDL services provide composition of algorithms and services based on the client request. But the privacy is not much studied for E-Services.

Mahmoud Awad and Larry Kerschberg [4] proposed a Service Oriented Architecture (SOA) for health information and here patients are "part owners" of their medical records and have complete ownership of their integrated health information. Here the new model of SOA is introduced for policy selection process in web service approach. In this implementation client's request for the single policy could not be satisfied by the user.

In the existing system, privacy platform preferences are focused mainly for major privacy policies. This privacy polices handled only a set of privacy rights and data in the web service platform. The individual data are not maintained with personal privacy for each access in the data providers. The analysis methodology is also not able to save a huge amount of privacy information of each individual. More than one factor may satisfy clients' trust preferences. To support the clients in the selection making, we promote various polices with different trust level. Limited access of data enabled with secret key and highly protected data transfers are done with security questions[5]. It defines the access of privacy policies in different stage with different security questions. It helps users to share high risk data with privacy for lifelong with more private policies.

Proposed System

In the proposed system, REST Webservice is used to view all sensitive information[6]. REST Communicates with the database and plays a vital role in retrieving the data and also acts as an interoperable interface between database and privacy related mechanism. Model-View-Controller (MVC) for implementing the above interface. Following are the remedies for the existing systems.
Remedy1(ForChallenge1): Dynamic Secret Key Generation
Remedy2 (ForChallenge2): Administrator who tracks all web crimes
Remedy3(ForChallenge3): CompatiblePrivacyPolicies (Security levels, ViewPrivacy, ViewQuery, Mean time failures, ViewQueryResult)

III SYSTEM ARCHITECTURE

The system Architecture of this privacy enhancement provides mechanisms for trust factor by establishing secret key as shown in figure 1. The web service polices build relationship trust via client and server. The secret key mechanism enables security mechanism including the access of policies and exchange of tokens in the trustful communication[7]. Authentication blog controls the overall process to ensure the trust factor for clients to access the web service polices.

The Architecture is implemented by using Microsoft .Net Platform. The .Net framework supports WS- Security and WS- Polices used by web services in the dynamic environment. GUI is also introduced to assist user to register the trust polices with different authentication factors. The privacy enhanced trust factor also provides identification of cyber crime scammers. It helps to build the high trust factor towards clients for web service. The cyber security is mainly applied for the subsystems in the health care application in the medical environment includes hospital, medical allowances, E-Record, Billing involves high trust factor. The arrows represent the flow of information or interaction between the modules.

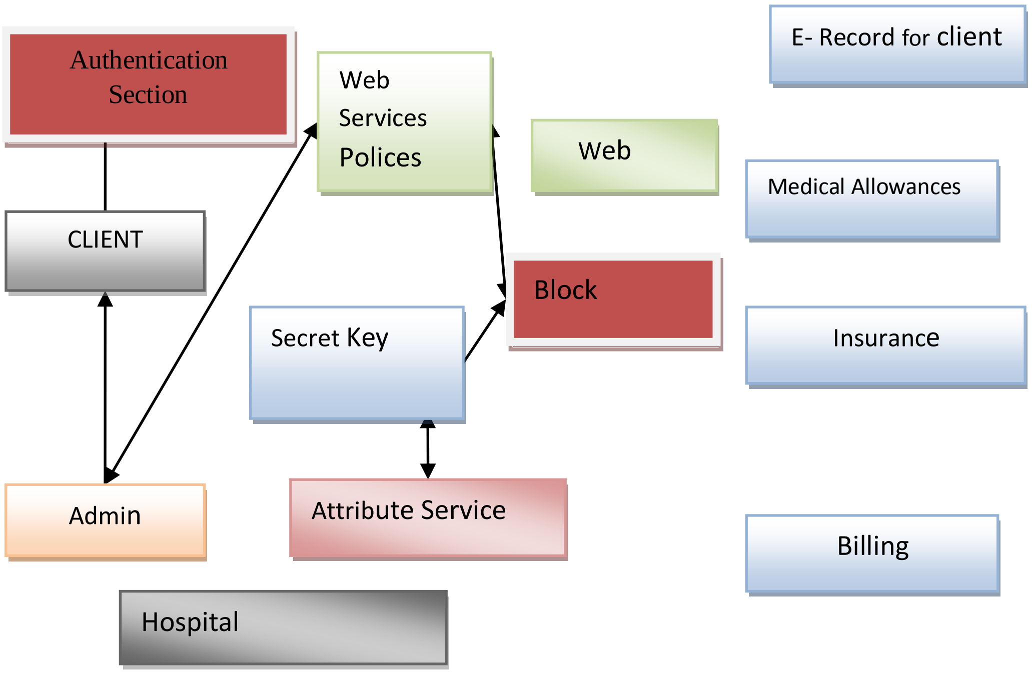


Fig. 1 System Architecture

The final stage is the secret key generation for all the interactions. The secret key is enabled for both the security domains and modules in the security domain. For efficiency, we use finger print and security questions after the generation of secret key in the modules interaction which helps to avoid the access of web services polices by scammers.

The workflow process is described from the steps 1 to 10.

1. After receiving policy request from clients service provider initiates request to server to access the policy from the different attributes corresponding to the clients trust factor. The security token is then verified to check the identity proof.
2. When the system receives request, secret key is generated to verify the user authentication and register the web service polices in its own domain.
3. Then the system verifies trust factor to the user's secret key and encrypt the policy request and send back to the server.
4. After receiving the acknowledgment the client checks the policy is accessed by the server side or not and again sends the request to the server to register for polices which the user wants to obtain from the medical record[8].
5. register() – Here the registration of the new users are submitted to the database. The registration process handles users details and security privileges.
6. user_authentication() – Here the system checks for valid username and password of the user.
7. admin_authentication() – Here the admin login credentials are been processed.

8. set_privacy_rules() – Here the admin sets the rules/policies for the user.
9. secret_key_verification()- Here the system asks for the user to send correct key in order to view their information. When the server gets the encrypted secret key it embeds user's request and sends the acknowledgement
10. check_for_privilege() – In this method, the system checks for the user's privilege's granted by the admin.

IV ALGORITHM

Step 1 : Input: P0 Set of polices request by user U, Embedded with set of privacy policies of user PU, where P is the set of privacy policies.
Step 2 : Let Sk be the secret key. Let Privacy policy(P0…..Pn) be selected by the user with the set of user privilege.
Step 3 : Let P=I; #initiation of privacy policy. Let P0= 1≤0; U ={0, 1, 2,…n};
Step 4 : Set Sk= I;
Step 5 : Q=Empty # Q is a queue contains polices to be selected.
  S=Empty #S is a queue contains privacy privileges to be selected.
  P=s[i]≤0; Q[i]≤0;
Step 6 : Extract S[i]={0,1.,2,………..,n};
  Extract Q[i]={0,1,2,………...,n};
Step 7 : Pw={siUPi} # web service polices with web service privileges Pi.
Step 8 : U++ # privacy selection of next user in the stack list.
Universally Unique IDentifier(UUID) is used in generating secret key randomly. Code for secret key generation:

```
String secretKey = UUID.randomUUID().toString();
```

Example for secret key:
e21c1c6d-e2d3-4d0c-9d21-ef8a054a62ac (32 bits)

V PRIVACY EVALUATION

Privacy evaluation matches the user's privacy requirements and the functional components at different privacy levels. The work flow of privacy model is shown in Fig.2. The main aim of the evaluation to identify the appropriate policy of each user in the dynamic web service environment[9]. The user preference is to hide their details and the communication from the third parties available in the same admin. For this purpose, specific security options to be set for each individual. The Algorithm defines the trust factor of privacy models and the privacy services to make the process simple for user to select their preferred policy from the stacks[10]. The sub process are also defined by the source of privacy evaluation with the unique secret key.

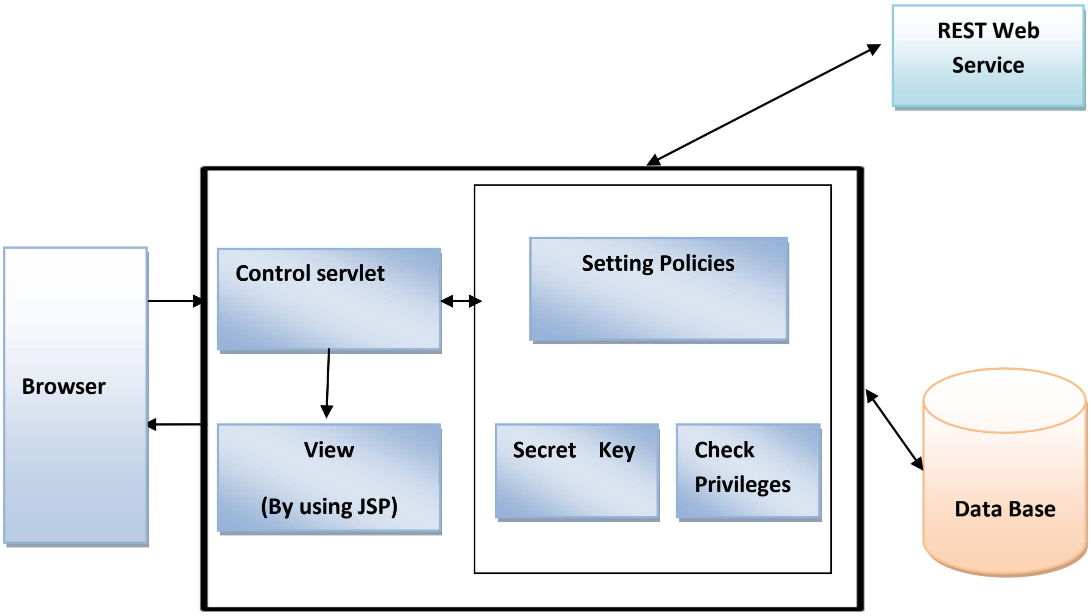


Fig. 2 Work flow of privacy model

Privilege represents the set of polices preferd by the group of users who communicate with the polices provided by the admin. The users have the direct communication with the policy provider in the WS environment. The trust relationships validate the policies in the old group and then verify the new service provider with the user primitives and requirements of the selected policy[11]. Fig.3 shows a sample policy document.

```
<?xml version="1.0" encoding="utf-8" ?>
<policyDocument
xmlns="http://schemas.microsoft.com/wse/2003/06/Polic
y">
<policies
xmlns:wssp="http://schemas.xmlsoap.org/ws/2002/12/sec
ext"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/poli
cy">
<wsp:Policy wsu:Id="trustlevelsec-token">
<wssp:SecurityToken wsp:Usage="wsp:Required">
<wssp:TokenType>http://www.contoso.com/tokens/custo
mXml#TrustLevelSecToken</wssp:TokenType>
<wssp:TokenIssuer>http://www.cs.virginia.edu/TrustLev
elSTS.ashx</wssp:TokenIssuer>
</wssp:SecurityToken>
<wssp:SecurityToken wsp:Usage="wsp:Required">
</wssp:SecurityToken>
</wsp:Policy>
```

Fig.3 Sample Policy Document

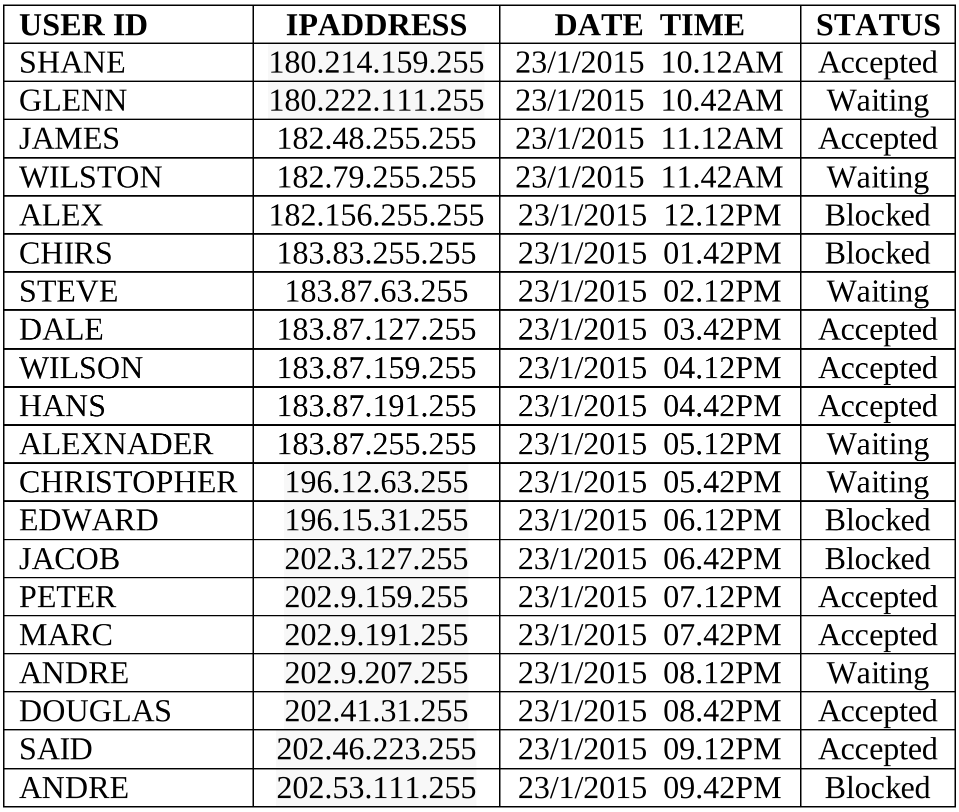
The interaction is completed with the disclose of user’s personal information through a web service. The privacy privilege specifies both the processing data to publish the declared privacy policy with the user’s satisfaction[12]. For privacy evaluation the following parameters applied as shown in Table I. Policies are set as the new user is registered to the system. When two services are composed the authorization is enabled if the matching frequency lieswithin two keys distribution. Layers of security for trust relationship is done in 3 levels.

Table I. Parameters Used

Parameter	**Value**
No. of policies updated	Once for every operation, Once when new user registered
Authorization check frequency through secret key distribution	2
Trust integrity threshold level	3

VI EVALUATION RESULTS

The project development and implementation is done in Eclipse platform with JAVA using MVC (Model View Controller) pattern. Based on the stated conditions the policies are enforced to make trusted service compositions and the privacy violations are trapped. A sample screenshot of the privacy violations trapped are shown in Fig.4. In this, there are three status of users trying to access the system are shown.



USER ID	IPADDRESS	DATE TIME	STATUS
SHANE	180.214.159.255	23/1/2015 10.12AM	Accepted
GLENN	180.222.111.255	23/1/2015 10.42AM	Waiting
JAMES	182.48.255.255	23/1/2015 11.12AM	Accepted
WILSTON	182.79.255.255	23/1/2015 11.42AM	Waiting
ALEX	182.156.255.255	23/1/2015 12.12PM	Blocked
CHIRS	183.83.255.255	23/1/2015 01.42PM	Blocked
STEVE	183.87.63.255	23/1/2015 02.12PM	Waiting
DALE	183.87.127.255	23/1/2015 03.42PM	Accepted
WILSON	183.87.159.255	23/1/2015 04.12PM	Accepted
HANS	183.87.191.255	23/1/2015 04.42PM	Accepted
ALEXNADER	183.87.255.255	23/1/2015 05.12PM	Waiting
CHRISTOPHER	196.12.63.255	23/1/2015 05.42PM	Waiting
EDWARD	196.15.31.255	23/1/2015 06.12PM	Blocked
JACOB	202.3.127.255	23/1/2015 06.42PM	Blocked
PETER	202.9.159.255	23/1/2015 07.12PM	Accepted
MARC	202.9.191.255	23/1/2015 07.42PM	Accepted
ANDRE	202.9.207.255	23/1/2015 08.12PM	Waiting
DOUGLAS	202.41.31.255	23/1/2015 08.42PM	Accepted
SAID	202.46.223.255	23/1/2015 09.12PM	Accepted
ANDRE	202.53.111.255	23/1/2015 09.42PM	Blocked

Fig.4 Privacy Violations Status

Genuine users are allowed to share information through service requests and compositions and their access status is referred as ‘Accepted’. When a suspected user tries to access the resources and if they do not possess the credentials to view sensitive data, they are marked as ‘Waiting’ and are to be approved by administrator. Those users violating the privacy policies by making changes to ownership or possessing unidentity, the status is set as ‘Blocked’. Different number of user groups are allowed to access the system with different credentials and privacy violations are studied. Fig.4 shows the different status of access to the system.

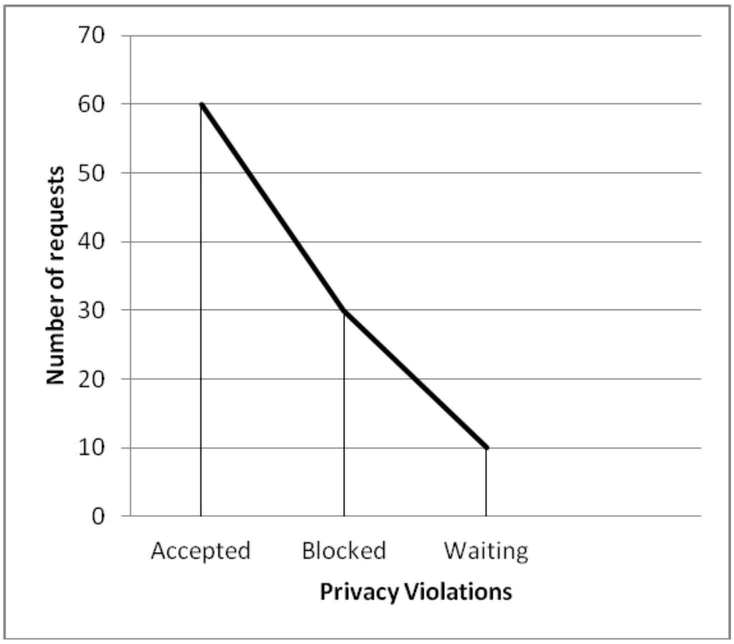


Fig.5 Status of Sample Requests

VII CONCLUSION

All health care data are to be more confidential and sensitive for the healthcare authorities. Especially, when information shared from one application to another, there is a possibility of leaksge of information. This may happen through hackers. When services are composed together, the privacy of data and its security must be ensured. In this paper, a privacy related mechanism has been proposed for accessing the health care data in a secured and privacy enhanced manner. With respect to REST approach different policies are selected on the basis of user information. The unauthorized users are blocked by the admin to rise the trust factor accessibility of user. e-Medical report evaluate the new generation of trust factor for all user to share their health information secretly with others. To increase the privacy performance REST module is used to categorize user's details(disease and other helath related information). Results show that the security level is highly trusted by applying privacy policies and the algorithms.

REFERENCES

[1] Sabrabeebe, Ms M., and Ms C. Nancy Nightingale. "Protecting Web Service Composition From Privacy Attacks Using Dynamic Privacy Model", International Journal of Innovative Research in Computer and Communication Engineering, vol.2, sp. issue 1, pp.2688-2694, (2014).

[2] Mohammed, Noman, et al. "Privacy-Preserving Data Mashup." Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, (2009).

[3] Salah-EddineTbahriti, Chirine Ghediraet.al., "Privacy-Enhanced Web Service Composition" IEEE Transactions on Services Computing(Vol.7, Issue 2), pp. 210-222, (2013)

[4] Mahmoud Awad and Larry Kerschberg, "Patient-Centric Secure-and-Privacy-Preserving Service-Oriented Architecture For Health Information Integration and Exchange Center For Health Information Technology", Center for Health Information Technology George Mason University, pp. 50 - 56, (2010).

[5] Shailesh Kumar Shivakumar, "Architecting High Performing, Scalable and Available Enterprise Web Applications", Elsevier store, (2014).

[6] Alrifai, Mohammad, Dimitrios Skoutas, and Thomas Risse. "Selecting Skyline Services For QoS-Based Web Service Composition." Proceedings of the 19th international conference on World wide web. ACM, (2010).

[7] A. Gil, W. K. Cheung, V. Ratnakar, and K. kin Chan. “Privacy Enforcement In Data Analysis Workflows”. In PEAS, (2007)

[8] Mahmoud Barhamgi, Pierre-Antoine Champin, Djamal Benslimane, Aris M. Ouksel, "Composing Data-Providing Web Services In P2P-Based Collaboration Environments”, Advanced Information Systems Engineering, Vol. 4495, (2007), pp.531-545

[9] Ashwin Machanavajjhala , Johannes Gehrke , Michaela Götz, “Data Publishing Against Realistic Adversaries”, Proceedings of the VLDB Endowment, v.2 n.1, August (2009)

[10] Berners-Lee,T.,Hall, W.,Hendler,J.,O’Hara, K.,Shadbolt, N.,Weitzner, D. “A Frame work For WebScience.” Foundation and Trends in Web Science,Vol 1,No 1(2006)

[11] Barhamgi, M, et.al, "A Query Rewriting Approach For Web Service Composition", IEEE Transactions on Service Computing, Vol.3, Issue 3, pp. 206-222, (2010).

[12] Gil,Y.,Ratnakar,V.,Deelman,E.,Mehta,G.and Kim,J.:Wings for Pegasus:”Creating Large-Scale Scientific Representations of Computational Workflows.Proceedings” of 19th Annual Conference on Innovative Applications of Artificial Intelligence(2007)