A Secured Web-based Health Care Platform Incorporating Naïve Bayes Classifier

K.R. Sarumathi
PG Scholar
Dept of CSE (PG) - ME (Software Engineering)
Sri Ramakrishna Engineering College
Coimbatore, India

R. Kanagaraj
Assistant Professor
Dept of CSE (PG) - ME (Software Engineering)
Sri Ramakrishna Engineering College
Coimbatore, India

ABSTRACT

Service computing is a cross discipline that covers the science and technology of bridging the gap between Business services and IT services. The demand for health care services motivated the creation of PHISP: a Public-oriented Health care Information Service Platform, where, service computing and related technologies are used. PHISP supports many health care services and provide guardianship. The intention is to create models of composite services to individuals through various key techniques of service composition supporting branch and parallel control structures. Security and semantic retrieval is an important issue for such a health care platform. The Boneh–Lynn–Shacham signature scheme improves the security by allowing the user to verify that the signer is authentic and the Elgamal signature technique for encrypting the stored data. The Ontology and naïve bayes classification algorithm has been utilized to increase the performance of the system. The experimental result improves the security and meanwhile, by using ontology and bayes' theorem the accuracy of the result is increased.

Keywords

Service Oriented Architecture, Service Composition, Web Services, ELgamal Signature, Boneh- Lynn – Shacham Signature, Ontology.

1. INTRODUCTION

In the past few years the population is increasing rapidly and the patients are also increasing which in turn increases the medical expenses and hence the need for the quality of Medical services are common nowadays. In order to improve the medical care, Information technology should be deployed in this field. In recent years there is a great increase in the medical care and the quality of the medical services are enhanced which in turn reduces the medical expenses. The remote health care facility increases the services to the patients. The importance to Medical Informatization has increased in various countries. Previous research in the field of medical health care and product development include 1) Informatization for medical records within the organization and regional health care information system 2) Digital Imaging and Communications in Medicine (DICOM). However there are some health care systems for the general users.

Health care systems (HCS) are the model of medical and health care services which are represented individually. Due to the enhancement in the medical field and the increase of medical patients, the health care systems should be gradually converted to a centralized treatment based model which holds few medical services. HCS model improves the services by providing personal health assessment and recommendation of health care services and so on. They provide health care services and medical prevention which can be enjoyed in their daily lives. A new computing model which is a user centric model is coming into existence which increased the service facility to the users; the model changes the original business model.

The service computing plays an important role in modeling medical services. The existing architectures were simple application architectures and not the modern architectures. The service oriented architectures (SOA) are not packaged in the form services and hence many functions cannot be performed. The service computing changes the original business model.

As the environment changes dynamically the application could not meet the diverse and personalized needs of the user and hence the active recommendation could not be provided for the users. Therefore under the new service computing scheme, remote medical health care services can be provided.

The main issues in these types of systems are security and privacy. There are many authentication schemes available such as password, finger print, iris scan, etc. In order to provide security to the system encoding schemes can be used. Ontology which provides efficient retrieval of the data and the classification and prediction methods improve the accuracy of the system.

Automatic service composition technique in service computing provides automatic composition of the related services needed for the users query. Classification technique improves the accuracy of the result provided to the users.

2. RELATED WORKS

Sirin *et al.* present a semiautomatic method for web service composition. Each time when a user requests for a service, all possible services which matches the requested service are displayed to the user.

Daniela Berardi: The web service composition is focused. There were many e-services that were in execution. These services were represented in the form of finite state machines. The complexity in composition of the services were analyzed and developed algorithms for composition, which work on all the e-services and respond with a single composite model of the services based on the request. This was the first algorithm written for service composition which was done automatically. Unfortunately, this could be used for real world applications.

Danilo Ardagna and Barbara Pernici: The service oriented applications use composition algorithms for creating models for e-services. Here there is an introduction to a new modeling approach where web service selection problem for large processes based on the quality of service constraints. The user preferences are taken into consideration and the service selection is performed dynamically. The constraint in the current implementation is that when request arrives for a single best service then the quality of service could not be achieved.

Seog-Chan Oh: To achieve the interoperability between the applications and to use the web services in a large scale networks, here they have considered service composition which was an error prone and difficult process. When the number of when services increases, finding the right service for satisfying the user preferences could not be satisfied. The AI framework is used and the composition is done considering the user preferences.

PengWei Wang.et.al, present a platform called Public-oriented Health care Information Service Platform (PHISP) under the new computing model, which supports several health care tasks and provide individuals with many intelligent and personalized health care services.

Here the platform is designed based on the modern SOA, which adopt Web services and the related composition technologies for implementation. The service composition using branch and parallel control structures is used for the composition of services. There is a security issue. Hence the performance of the system should be increased and also the security should be improved.

3. EXISTING SYSTEM

3.1 Web service creation

Web service creation is the first step, where the services related to health care such as health guidance, Environment, Medicine, Geographical, diet, etc, are created. The web services are created based on the medical related data which is taken in the form of a dataset. The case study on the medical information can be done and converted in the form of a dataset.

3.2 Registration and requisition

The user registers enter in their name along with their personal and basic medical details for accessing the service. Once the user is registered using their username and password could enter into the system and request for the necessary services. The request consists of the query containing the disease type and the basic medical information's such as blood group, etc. The corresponding service requests are then sent to administrator.

3.3 Administrator

Administrator has its own password to login to the server and they process the request sent by the user. The Process of service selection and composition is done by considering the user preferences. The service composition using branch and parallel control structures algorithm is taken for generating results for the query.

4 PROPOSED SYSTEM

The proposed work mainly concentrates on improving the security and efficient retrieval of services related to user request. User sends a request to server and that request is encrypted using BLS algorithm and stored in the database.

In cryptography, the Boneh– Lynn–Shacham signature (BLS) scheme allows a user to verify that a signer is authentic. Digital signature is one of the most important cryptographic primitives. In traditional public key signature algorithms, the binding between the public key and the identity of the signer is obtained via a digital certificate. Server verifies the user and retrieves the request and decrypt to get original request from the encrypted format. The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography, which is based on the Diffie–Hellman key exchange. The ElGamal signature algorithm is used for encrypting the users' medical records. Ontology is used, which makes searching easier.

Ontology is the philosophical study of the nature of being, becoming, existence, or reality, as well as the basic categories of being and their relations. The ontology improves the searching easier and this is useful when we move for large datasets. The information is represented in a tree structure. The tree is displayed only when the admin enters the key value of the particular user. The tree structure consists of the basic information along with the medical details.

4.1 The Boneh–Lynn–Shacham signature scheme

The Boneh–Lynn–Shacham signature scheme (BLS) is used for encrypting the user login information and the requisition details entered by the user. This algorithm verifies whether the user is authentic and then allowing them to access. It also has the limitation up to three tries.

– KeyGen: Let H: {0, 1} ↑* G1 be a Map-to-point hash function.

– The secret key is x□RZ→q. and the public key is Ppub = xP for a signer.

– Sign: Given secret key x and a message m €{0, 1} ↑*, compute the signature σ= xH(m).

– Verify: Given public key Ppub = xP, a message m and a signature σ, verify e(P,σ) =e(Ppub,H(m)).

4.2 Key generation based on ElGamal signature scheme

Elgamal signature method is used for encrypting the user medical records along with their basic information. The private key generated in this algorithm is used for authorization of the user, once the admin provides the private key for the particular user; the ontology tree can be viewed by the admin, which improves searching. The medical records are encrypted and stored in the form of a dataset and the decryption process is done

The signer performs the following steps to sign a message m,

Sender Chooses random k

Chooses private key X, Prime p and generator g, public key of receiver Y = gx mod p is calculated.

Calculate K = Yk mod p

Calculate C1= gk mod p C2=M K mod p

Calculate C1x mod p = K and recovers message M = K-1C2mod p, K-1= the inverse of K mod p.

To decrypt a cipher text (C1, C2) with the private key X

M= C2 / C1 ^x mod p.

Where M= Message.

4.3 Classification

The dataset containing the medical details of the diseases are classified by applying the bayes' theorem with independence assumptions. Naïve Bayesian classifier exhibit high accuracy and speed when applied to large databases. The assumption made by this classifier is called class conditional independence.

Conceptually, the probability model for a classifier is a C1 conditional model is given as,

$$P\ (C|\ F1,\ldots\ldots,Fn)$$

Over a dependent class variable C with a small number of outcomes or classes, conditional on several feature variables F1 through Fn. If the number of features n is large or when a feature can take on a large number of values, then supporting such a model on probability tables is insufficient is the main problem. We consequently reformulate the model to make it more tractable. The dataset is taken as input and the probability values are taken to classify and predict the disease to which it belongs.

Using Bayes' theorem, it can be written

$$p\ (C|\ F1,....,Fn) = \frac{p(c)p(F1,.....Fn|c)}{p(F1,....Fn)} \qquad (1)$$

5. EXPERIMENTAL RESULTS

The Performance of the system is evaluated by considering security as the parameter. The proposed system is compared with the existing system [21] at the security level. In the following graph, x axis denotes the records and y axis denotes the security level. The proposed system has more security level when compared with the existing system.

In other words, proposed system is a well secured system. In the instance, security level value of the proposed system and existing system are 85.52 and 60.50 respectively. Introducing the cryptography in the existing system improves the security.

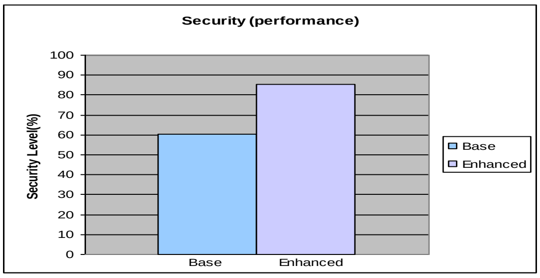

Fig. 1 Security level comparison

Table 1. Comparison Table

X-axis	Security level
Base	60.50
Enhanced	85.52

6. CONCLUSION AND FUTURE WORK

The previous works in the literature in the field of health care demanded for the services, based on which a Public Oriented personalized health care platform has been designed. The service composition using branch and parallel control structures has been used in creating the composite models of the services. To resolve the security issues and to improve the performance of the system we go for the Boneh–Lynn–Shacham signature scheme, for securing the authentication and personal details of the user and Elgamal technique, for encrypting the response messages to the users. The response messages include the user's medical records. For easy retrieval of the information, we go for ontology, which generates OWL file. To increase the performance of the system we go for Naïve bayes classification, where the category of the disease is predicted based on the probability value. The Experimental result shows that our proposed work improves the performance and the security of the platform is enhanced. Further improvement of the system can be done by using some other security techniques and the classification algorithm.

7. REFERENCES

[1] PengWei Wang, ZhiJun Ding, ChangJun Jiang, and MengChuZhou, "Design and Implementation of a Web-Service-Based Public-Oriented Personalized Health Care Platform", IEEE trans. on systems and cybernetics: systems, man and cybernetics, VOL. 43, NO. 4, JULY 2013.

[2] Aviv Segev and Quan Z. Sheng, "Bootstrapping Ontologies for Web Services", IEEE transaction on service computing, VOL. 5, NO. 1, pp. 33-44 Jan-Mar 2012

[3] Z. Duo, J. Li, and X. Bin, "Web Service Annotation Using Ontology Mapping," Proc. IEEE Int'l Workshop Service-Oriented System Eng. (SOSE '05), 2005.

[4] S. C. Oh, D. Lee, and S. R. T. Kumara, "Effective Web service composition in diverse and large-scale service networks," IEEE Trans. Serv. Comput., vol. 1, no. 1, pp. 15–32, Jan.–Mar. 2008.

[5] Li Xiao-fei, Shen Xuan-jing, Chen Hai-peng, "An Improved ElGamal Digital Signature Algorithm Based on Adding a Random Number," Proc. IEEE Int'l Conf. on Services Computing (NSWCTC '10), pp. 236-240, 2010.

[6] [6] D. Ardagna and B. Pernici, "Adaptive service composition in flexible processes," IEEE Trans. Softw. Eng., vol. 33, no. 6, pp. 369–384, Jun. 007.

[7] Liu, J.N.K., Li, B.N.L., Dillon, Tharam S., "An improved naive Bayesian classifier technique coupled with a novel input solution method [rainfall prediction]" IEEE trans., Man and cybernetics: Systems, VOL. 32, NO. 2, pp. 249 – 256, May 2001.

[8] E. Sirin, J. Hendler, and B. Parsia, "Semi-automatic composition of Web services using semantic descriptions," in Proc. Web Services: Model., Arch. Infrastruct. Workshop ICEIS, Angers, France, Apr. 2003, pp. 17–24.

[9] S. C. Oh, D. Lee, and S. R. T. Kumara, "Web service planner (WSPR): An effective and scalableWeb service composition algorithm," Int. J. Web Serv. Res., vol. 4, no. 1, pp. 1–23, 2007.