PRIVACY ENHANCED PERVASIVE MODEL WITH DYNAMIC TRUST AND SECURITY IN HEALTHCARE SYSTEM

[1]GEETHA MARIAPPAN AND [2]MANJULA DHANABALACHANDRAN

[1]Department of CSE, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India

[2]Department of CSE, CEG, Anna University, Chennai, Tamil Nadu, India

E-Mail: geethapandian@yahoo.com , manju@annauniv.edu

ABSTRACT

In Pervasive environment privacy is foremost concern. In this paper proposed an intelligent mechanism for privacy preservation model using dynamic trust and security management techniques. The minimum required information without ambiguity to be extracted from the trusted store and is to be conveyed or exchanged to the trusted entities with in or outside the system as many times as possible in the right context during right session to enhance the privacy of the information. Here the issue is concurrency and asynchronous nature of the information that means the same information is to be retrieved by the number of entities at the same time during any session. So, the availability of the user information and displaying secret information in public centers will create a negative impact on some important users. To avoid this scenario we develop an intelligent system which can identify trusted entities and dynamically adopt a mechanism in relation with other contextual entities.

Keywords: *Privacy, Data Globalization, data Virtualization, Data embellishment, Pervasive*

1. INTRODUCTION

Networking technology is essential tool for everyone's day to day activities , various individuals, different companies and an organizations which are increasingly depending on an electronic devices used to process information and to avail services trough an intelligent way in pervasive computing environment. While doing so, sensitive information will definitely be a problem of privacy[1]. So that third party cannot access the sensitive data without any trust provided by network. Given this micro data , privacy already been measured by k_anonymity[2], l-diversity[3], differential privacy[4], t-closeness[5] and Blend me in[6]. But all of these measures having some limitations to produce significant result expected. To avoid the above said measures along with Blend me in technique we propose a model measuring privacy while data is revealed to third parties mechanisms to improve the privacy of pervasive environment. The health care system needs an enhanced privacy model satisfying the needs of various stake holders with different policies at different time period. The collaborative approach and strategic reasoning in managing the trust across them with the security measures devised and implemented during information processing as well as communication activities determine the confidentiality of health information. The platform over which the actors play their role and the mis-useses that are not permitted over any session of interaction govern the other attributes of privacy like pseudo anonymity and unlink ability. The uncertainties involved in the trust management due to random failure of the devices and security faults in the system design may decrease the privacy. The privacy in the health care domain seeks compliance with portability of insurance information and its accountability once the information needs to be migrated into other domains. A trust-based security model[7] for the collaboration between devices within pervasive computing environments ensures a secure interaction between smart devices and services, by addressing the security and trust. And also identifies security problems of accuracy of personal information and trust .Privacy criterion compares users' perception and confidence in the way their information is stored and exchanged. It also compares the degree of risks in compromising the privacy of user information [5]. Because of higher risk of losing the user's device, the risk of identity thefts is in pervasive computing is high.[8].

Privacy concerns what kind of data we are going to protect except dark data across many different communication gateways, Where this data is and properly classify it, How this will be protected using protocols. And also it needs balance between security and usability. Traditional model requiring users transparent input have to be replaced with the system and this can protect the sensible information securely and automatically from the system in a pervasive environment to other communicative devices and users. This gives users control over the release of their information in the pervasive environment that can reflect the misuse of sensible information by others[9],[10]. To protect privacy of user's sensible information we propose a method g-anonymity focus on the following techniques such as Data Globalization, Data Virtualization and Data Embellishment.

2. PROPOSED MODEL

K anonymity approach faces a setback in the case of deployed macro data since the anonymity is expressed towards micro data table. The pervasive privacy can be achieved through the implementation of g- anonymity is that is based on Data Globalization, Data Virtualization and Data Embellishment(*Fig 1*).

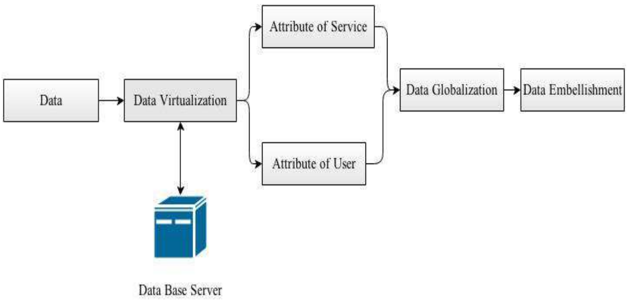

Fig 1:Trust And Privacy Data Model In Pervasive Environment

2.1 Data Virtualization

Data Virtualization is an abstract view of data. It contains collection of dataset. All the data virtualized from the table. Virtualized data in a table may be thought of as an added field or diminished field in the original master table, so that each tuple representing unique data as in the original master table. The mapping between original and replicated data is done by a careful data enriches so that not more than V sets have same fields. A *Fig 2and 3* shows a case study to demonstrate the data virtualization in health care management system and its entities.

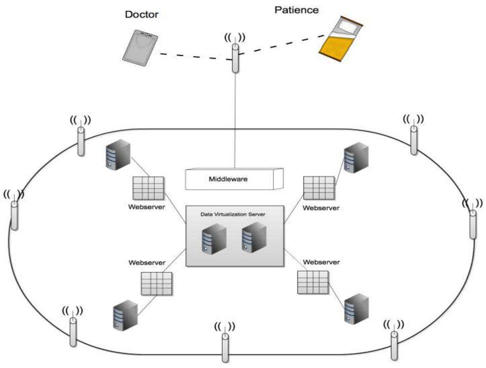

Fig 2: Data Virtualization In Health Care Management System

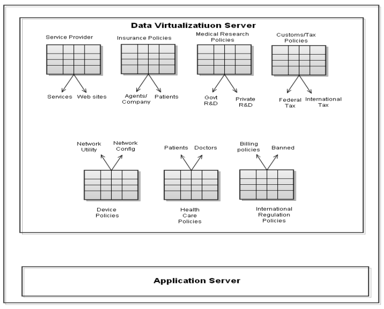

Fig 3: Data Virtualization Server

For example, patient's prescription may be defined in original database as

$$\textbf{Prescription} = \mathbf{P_{ij} . D_{xy} . T_{dt}},$$

Where P_{ij} is the Prescription of j^{th}Patient given by i^{th}doctor, D_{xy} is *ax* number of times ,*y* quantity of dosage D Given to the Patient, T_{dt} is Treatment T given on indicated date *d* at time *t.*

After virtualization, the prescription of the same patient may be defined in virtualized table as Duplication of Prescription of $\mathbf{P_{ij}' \cdot D_{xy}' \cdot T_{dt}'}$ **. As** we know that the updation of virtualized table contents will not affect the original table, Information misuser and eaves dropper as mentioned below cannot enter the place of hacking.

Eaves Dropping= $P_{ij}{}^{”} \cdot D_{xy}{}^{”} \cdot T_{dt}{}^{”}$

Information misuse=$P_{ij}{}^{’’’} \cdot D_{xy}{}^{’’’} \cdot T_{dt}{}^{’’’}$

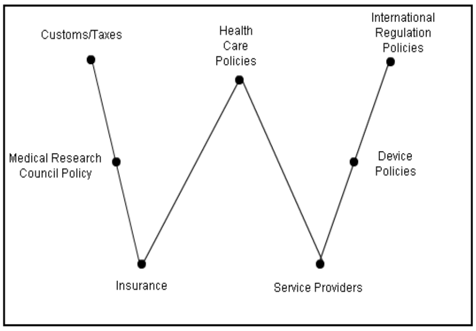

Fig 4: Health Inter related Policies (VV Model)

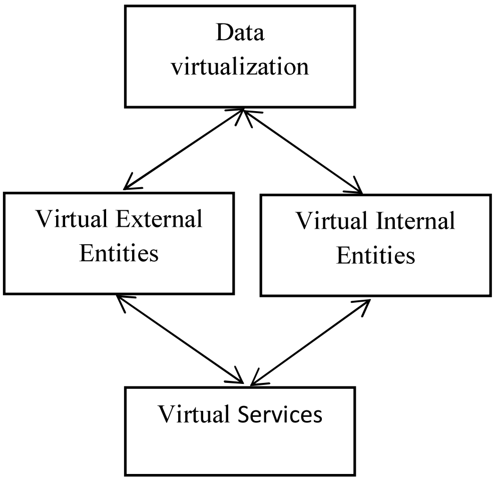

Fig 5 : Dynamic Trust Management framework

2.1.1. Dynamic trust engine for healthcare entities:

The anonymity and unlinkability issues can be solved by introducing a virtual index of the services during the session along with their most common attributes. This can be explained by the algorithm of *“Virtual Identity of services and attributes”.*

2.1.2. Virtual identity of services and attributes(visa algorithm).

Physical services: a^{p0}, b^{p0}, c^{p0}, d^{p0}

a^{p0} is a deployed deliverable operational physical service or the original deployed code running in the parent physical server. Similarly, b^{p0}, c^{p0} , d^{p0}, e^{p0} are heterogeneous serviced checked for their compliances and deployed in different servers or in a single server.

a^{p0} is mapped with number of virtual services shown in *fig 5* using application or service virtualization to say “l” number of services, a^{11}, a^{21}, a^{31}, a^{41}…….. a^{l1} that are operational and deliverable.

In the similar way, b^{p0} is mapped with number of virtual services using application or service virtualization to say “m” number of services, b^{11}, b^{21}, b^{31}, b^{41}…….. b^{m1} that are operational and deliverable. $c^{p0}$is mapped with number of virtual services using application or service virtualization to say “n” number of services in which some of them are operational and some are suspended services.

Physical services are patient identification service, authentication service, billing service, emergency service, first aid service and ambulance service. These information can be obtained through the interaction of mobile application interface with the web server so as to respond to the incoming queries. Since more number of similar requests from heterogeneous clients are coming at the same duration, it is essential t0 virtualizes the services and deploy them in different servers based on the geographic specification of the healthcare data center. Each and every service is having different attributes and in some occasions, a single service may have different attributes while deployed in different areas. Hence the identification of the correct service to the needed client who demands the expected attributes of that service has to be identified. It is a complex process when more number of requests are entered from the same client in different timing. The correct mapping of the patient request towards the services and their attributes are to be checked using the proposed VISA algorithm where the indexing is done virtually that is a logical mapping is achieved based on the similarity of the requests and the attributes. The status of the service whether it is in the deployable status or not is to be checked and then the quality attributes of that service as expected by the requester are to be verified before rendering them in the right time. The identification of the service among a pile of stacked services are shown in *Fig 6*. The authentication and authorization of that client or administrator to utilize the service is also to be checked as per the policy (shown in *Fig 4)* of the service provider. The integrated tax policies, legal policies and the insurance policies are to be rendered with maximum security if only if the patient is a trustable entity with respect to the party who involved in that transaction.

Virtual Services: $a^{11}, a^{21}, a^{31}, a^{41}........ a^{l1}$
$b^{11}, b^{21}, b^{31}, b^{41}....... b^{m1}$
$c^{11}, c^{21}, c^{31}, c^{41}........ c^{n1}$
$d^{11}, d^{21}, d^{31}, d^{41}....... d^{r1}$

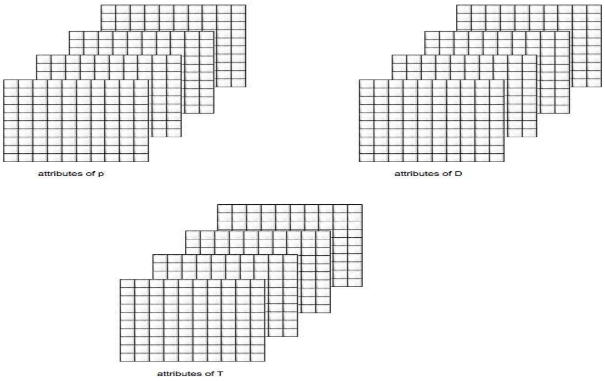

Fig 6: Data Virtualization and its attributes

The Healthcare Service category S can be defined as **S= (G, L, Q,P)** // G-generic, L-location, Q-quality,P-policy)//

Where G is Generic and it can be defined as

Generic::generic(serviceid,service_name,

service_interface)

L is location and it can be defined as

Location specific::loc-specific(geo, radius, handover, protocol)

Q is quality and it can be defined as

Quality specific:: qual_specific (cost, availability, performance)

and P is policy and it can be defined as

Policy specific::policy_specific(integrity, privacy, recoverability).

Other parameters of this deployment are,

Deployable: Boolean : True | False

Undeployable: Boolean: True | False

Status: Deliverable, Terminated, Suspended,

Operational

Accountable: Public, Private, Hybrid

Return on Investment: Deployment Cost, Maintenance cost, Revision cost, Resource utilization cost Operational Cost, Exceptional Charges, Savings on Time

Service: Physical | Virtual

Number of Services: *num-ser*

Base name types for services: Nat , Boolean

where Nat is Natural number.

The constructed types are **list** and **set.**

If a group of services which are entities are interacting, it is possible to consider a list of services or a set of services for future composition. The set does not focus the *order* of the elements whereas the list type forces a strict order of its elements to process. In a service composition model, if one service is *activated* to *interact many times* with a number of other deployed services in different servers, the basic data types used are as shown:

Activated: Boolean

Times of interaction: Nat

In another scenario, by interacting with one fault free service, if a virtual service returns the needed service within the specified time, then the same service is reliable otherwise unreliable and so can be terminated or suspended. The status of the services are transitive and symmetric so that the composition of a list of named services can be predicted.

Reliable, Available, Secured: Boolean

Reliability: Nat

The service x trust y and y trust z *implies* x trust z. That is the amount of uncertainty between these members is below the threshold value.

x trusts y and y trusts z→x trusts z

By applying the functions to the arguments, terms are generated.The term is having a type. The derived type of the term depends on the type of arguments to which the functions are applied. The terms may be Boolean type and it may have any abstractions based on the applications.

If a service is available then it is reliable else it is unsecured

If a product is compliant then it is permitted else it is stopped

The formulae are terms of the type Boolean and it is possible to declare some variables as free, bound and unknown variables or attributes .Usual logical connectives like Negation, AND, OR and Implies can be applied with decreasing order of priority to the terms with variables.

For example, if company1 and company2 collaborate in manufacturing a product and the company3 is having a sales agreement with company 2, then it may be specified as

Company1∧Company2→ Company3 or

Company1 → Company2 ∧ Company3 (Right associative)

Trust is in the broadest context can be considered as **acceptable uncertainty** about one entity perceived by other. It can be imagined as the arguments associated with any entity in that domain of interest.Trust is of a theory and can be considered as a bag of entity types, relations or functions of the entities with respect to other entities in that domain.If trust is existing, it is possible to have a Boolean type.

2.2. Data Globalization

Data globalization is the technique to substitute the values of sensible information with more common values. The virtualized data in a table may be thought of as an added field or diminished field in the original master table so that each tuple representing unique data as in the original master table. The mapping between original and replicated data is done by a careful data enriches. This is shown in *Fig 7.*

2.3. Data Embellishment

Data embellishment in elaborating or hiding the values of those information as many times as possible.

3. CASE STUDY

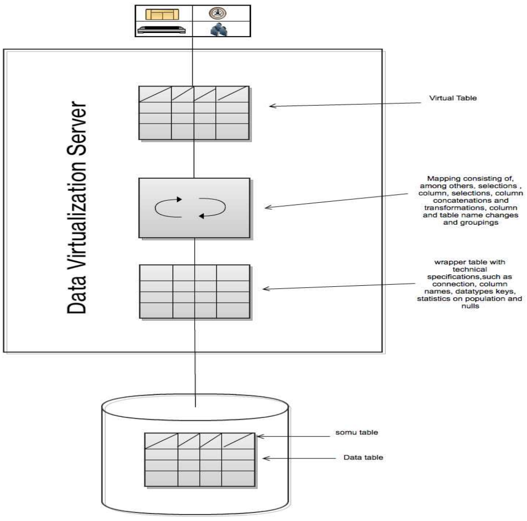
Data Virtualization Server
Virtual Table
Mapping consisting of, among others, selections , column, selections, column concatenations and transformations, column and table name changes and groupings
wrapper table with technical specifications,such as connection, column names, datatypes keys, statistics on population and nulls
somu table
Data table

Fig 7: Relation among virtual table, mappings, wrappers and source table

To Protect individual information from of a person(or record), Three Anonymization and virtualization techniques are used, They are: Globalization, In which the identity of the individual is protected by Globalizing certain field of the table, when the hackers tries to hack the individual information, all the get is a general view, with that information it is nearly impossible to hack the system, For Example: a database contains information of all the services provided by a Healthcare, by globalizing the deployment server (in which the service is deployed) field, we provide most Globalized(or common) form of the data, with this information, hacker cannot identify a particular field and the Second Technique is Virtualization, in this technique, the main database is not directly. .

Table 1: Software

No. of VM’s	3
Protocol	IPv4
Total RAM Size	1024MB
HyperVisor	Xen
Application Virtualization	XenApp
Softwares	.Net,SqlServer2005

Requirements

Table 2: Source table [values] and attributes

Service No	Service Name	Deployment of Server	Attributes of Services					Attributes of User				
			Cost/Hr	Platform	Physical/ virtual?	Private/P ublic?	Corporat e/Individ ual?	MAC Address	IP Address	device	Platform	Service Provider
1	&Alcohol problem service	Linux	200	open	virtual	Private	Corporate	02-AB-45-67-F0-B8	1.7.255.255	Mobile	Open	BSNL
2	Emergency care Service	Windows	300	Closed	Physical	Public	Individual	01-23-45-67-89-AB	1.23.255.255	PC	Closed	Airtel
3	Insurance and Plan service	Linux	200	Open	Virtual	Public	Corporate	00-B0-D0-86-BD-F7	1.39.255.254	PC	Open	Reliance
4	Trials and Information service	Windows	200	Open	Virtual	Public	Corporate	00-00-0C-60-8B-41	134.189.23.42	Mobile	Open	Tata DOCOMO
5	Medicare and Medic-aid service	Linux	200	Open	Virtual	Public	Corporate	00-80-5F-D8-A4-8B	134.189.23.42	PC	Open	MTS
6	Pharmacy service	Windows	250	Open	Virtual	Public	Corporate	00-80-20-88-83-57	255.255.248.0	Mobile	Open	BSNL

Table 3: Virtualized Table

Service No	Service Name	Deployment of Server	Platform	IP Address	device
1	Alcohol &Alcohol problem service	Wondows,Linux	open	1.7.255.255	Mobile
2	Emergency care Service	Windows	Closed	1.23.255.255	PC
3	Insurance and Plan service	Linux	Open	1.39.255.254	PC
4	AIDS clinical Trials and Information service	Windows	Open	134.189.23.42	Mobile
5	Medicare and Medic-aid service	Linux	Open	134.189.23.42	PC
6	Pharmacy service	Windows	Open	255.255.248.0	Mobile

Table 4: Globalized values of attribute "Deployment of Server"

Service No	Service Name	Deployment of Server	Platform	IP Address	device
1	Alcohol &Alcohol problem service	Operating System	Open	1.7.255.255	Mobile
2	Emergency care Service	Operating System	Closed	1.23.255.255	PC
3	Insurance and Plan service	Operating System	Open	1.39.255.254	PC
4	AIDS clinical Trials and Information service	Operating System	Open	134.189.23.42	Mobile
5	Medicare and Medic-aid service	Operating System	Open	134.189.23.42	PC
6	Pharmacy service	Operating System	Open	255.255.248.0	Mobile

Table 5:Result of Data Embellishment for the attribute "IP Address"

Service No	Service Name	Deployment of Server	Platform	IP Address	Device
1	Alcohol &Alcohol problem service	Operating System	Open	1.X.X.X	Mobile
4	AIDS clinical Trials and Information service	Operating System	Open	134.X.X.X	Mobile
6	Pharmacy service	Operating System	Open	255.X.X.X	Mobile

4. DESIGN AND IMPLEMENTATION

This script contains all the virtual machine configurations can use the following system requirements:

Processor: IntelCorei3M3302.13GHz and Mother Board: Intel5SeriesBoard3400SH .

Other software requirements are shown in *Table 1*. This can be accessed by the users, instead a Virtual Database with limited field accessibility is provided, that hides most of identity information from hackers, For Example(Given in *Table 2*), if in a situation, where services that are only to be accessed via mobile, are alone enough, in that situation a virtualization technique is applied to provide only those records with limited information(Shown in *Table 3*). The second technique Globalization is used to protect the valuws which are stored in original table.(Shown in *Table 4*). And the third technique is Embllishment, In which limited information (records) are provided, like virtualization and Certain fields are shown, but doesn't provide the full Value of that field(Shown in *Table 5).*

Sample mapping function given below is used to explain the g-ananomity with virtual services.

```
DEFINE V_SERVICE

SELECT

ServiceNo, ServiceName, Deployment of Server, Attributes of Services.Platform, Attributes of User.IP address, Attributes of User.device

FROM    SERVICE WHERE

Attributes of Services.Platform=”Open” and Attributes of User.device=”mobile”
```

5. CONCLUSION

The privacy mechanism developed in this study enables the both micro data and macro data to dynamically manage information privacy in pervasive computing environment and to define health care policies for all entities considering their trust and corresponding attributes with 100% accuracy and minimum time. This mechanism also offers protection against privacy threats existing in pervasive computing environments. Although the mechanism is targeted to pervasive healthcare, it can easily be modified to other services with different domains.

REFERENCES

[1] Qinghua Li, Guohong Cao, ‘Efficient and Privacy-Preserving Dta Aggregation in Mobile Sensing”, IEEE International conference on network protocols(ICNP), Oct.30-Nov.2 2012, pp. 1-10.

[2] Bandana kumari, G.Geetha, and L.Bhagyalakshmi, “K-anonymity based privacy-preserving location monitoring services for wireless sensor networks” , International Journal of computer applications in Engineering sciences, August 2013, vol-III, pp.151-159.

[3] A.Machanavajjhala, D.kifer, and J.Gehrke, “ l-diversity: privacy beyond K-anonymity”, ACM Transactions on Knowledge Discovery from data, 2007, pp.1-36

[4] N.Li and T.Li, “t-closeness: Privacy beyond k-anonymity andl-diversity”,Data Engineering,Vol. 2.

[5] C.Dwork, “Differential privacy: A survey of results”, Theory and Applications of Models of computation, 2008, pp.1-19.

[6] Alegria Baquero, Allan M. Schiffman and Jeff Shrager, “Blend me in: Privacy preserving input generalization for personalized online services”, Proceedings of the International conference on privacy, security and trust(PST2013), July 10-12, 2013.

[7] Pekka sakari Ruotasalainen, Bernd Blobel, Antto Seppala, and Prikko Nykanen, “ Trust Information – Based privacy Architecture for Ubiquitous Health” JMIR Mhealth Uhealth 2013, Vol.1, issue.2, pp.1-15

[8] Kui Ren, Wenjing Lou, Kwangjo Kim, and Robert Deng, “ A novel Privacy Preserving authentication and access control scheme for pervasive computing Environments” IEEE transactions on vehicular technology, 2006.

[9] Keke Chen, and Ling Liu “Privacy-preserving Multiparty Collaborative Mining with Geometric Data perturbation”, IEEE transactions on Parrallel and distributed computing, January 2009.

[10] Qi Xie and Urs Hengartner, "Privacy-preserving Matchmaking for mobile social networking secure against malicious users", International conference on privacy, security and trust,2011.

[11] Jiawei Yuan, and Shucheng Yu, " Privacy preserving Back-propagation neural network learning made practical with cloud computing", IEEE Transactions on parallel and distributed systems,2012.