A Policy and Trust-based Secure Communication Protocol in Information Systems

T.Chalama Reddy
Assoc Professor, Department of CSE,
Narayana College of Engineering,
Nellore, INDIA

R.Seshadri, PhD
Professor & Director, Computer Center,
Sri Venkateswara University,
Tirupathi, INDIA

ABSTRACT
Security in information systems has increased importance, as end users have become more responsive of securely sharing or exchanging the vast amount of information. The organizations that do sensitive work such as those with defense contracts, passport issuing agencies, military activities, and health care data at health-insurance, are in need of protecting their information. Nowadays, financial institutions providing various online services to customers are facing situation with customers who submit fake documents for getting services. To defend from that situation, financial institutions enquire customer information at various government departments against the customer submitted proof documents to rovide service to customer. In this study, secure and trusted information sharing environment is a vital requirement to make users interact and share data easily and securely across various networks. The prime challenge is to evaluate the trust of financial institution that characterizes secure information sharing in various government departments. The secondary challenge would be a development of communication protocol that securely exchanges information among various financial institutions and various government organizations. This paper emphasis on policy and trust-based secure protocol that offers confidential and authenticated, and trusted information sharing among financial institutions and government departments without creating any problems to information security by using cryptographic hash, private and public key encryption algorithms, and trust evaluation techniques. Furthermore, it facilitates non-privacy preserving information sharing with probable restrictions based on the rate of trust factor of financial institutions. This protocol assures that secure and stream- lined information sharing among financial institutions and government departments leads to avoid intimidating activities. The experimental results show the effectiveness of the proposed policy and trust-based information sharing approach.

Keywords
information security, information sharing, policies, trust factor, private and public key cryptography, Secure Hash Algorithm(SHA-1),Credit Information Bureaus of India Limited (CIBIL).

1. INTRODUCTION
With the development of computer and the communication technology, individuals and organizations are heavily depending on the availability of interconnected information systems for storing and communicating their valuable information. However, the presence of malicious attackers and careless users inside and outside the systems as well as on the interconnected computer networks is, at the same time, posing severe threats to our systems. These threats include eavesdropping for accessing confidential information without permission, malicious attacks and intrusion for destroying and preventing legitimate users from access the systems, or leakage of valuable information due to the misuse of the systems by careless users. To protect our system from threats, Information security is an enabling technology which allows us to protect our electronic assets and valuable information stored in our systems or transferred over computer networks from being damaged, stolen or misused by malicious attackers or careless users.

Government organizations maintain sensitive and confidential information for its operations. For example, personal details at governments, Health care data at health-insurance, defense contracts and military details are very sensitive information, when some information in government organizations should be shared with other organizations, risk of information drastically increases. The most of the information at government organizations are currently stored in digital form, when it is delivered to other parties through network. It can be very easily made copy, transferred to other persons, with a simple click of internet browser button, or modified for malicious purposes.

The basic requirement for a digital government is to act on the anticipation of its people to ensure the security for its data systems. Data security is safeguarding the data and data systems from unauthorized entrance, use, disclosure, disruption, alteration, or destruction. The security issues can be predictable by projecting it onto a three-level hierarchy: management level, system level, and data and application level. The major elements of data security involve integrity, privacy, availability, authentication which has to be taken into consideration at diverse levels within the hierarchy. Confidentiality is the property of precluding disclosure of data to unauthorized individuals or systems. Integrity implies that the data cannot be altered without authorization. Availability is that the computing systems used to store and process the data, the security controls used to preserve it, and the communication channels used to access it should be operating precisely [1].

In existing information sharing technologies, the main problem behind the attacks is poor security information sharing. For instance, in Mumbai attack, even after the coast guard had found out and that there might be an attack from the sea and if that information had been shared through a proper channel to the required agency, the attack could have been stopped. So, we find that there is no proper information sharing between intelligence agencies. Also even if there is a channel and during such information sharing from one agency to another the communication if not secure, may be forcefully hacked by the terrorists which will be a major value for enhancing the attack by the terrorist organizations. If there is a

proper secure information sharing technologies, they can share the information widely to the all Federal Agencies and reduce the possibilities of these attacks.

Nowadays financial institutions providing various online services to customers are facing situation with customers submitting fake documents for getting services. To defend from that situation, financial institutions enquire customer details at various government departments against the customer submitted proof documents to provide service to customer. Developing a secure and trusted information-sharing protocol in between and among financial institutions and government organizations is the primarily motivation behind this research work. To make a broad foundation for data sharing needs trust among all data sharing partners. The trust based data sharing technologies are controlled by Digital Government and it is referred as Trust Management. There exist currently two different major approaches for managing trust: policy-based and reputation-based trust management. These approaches have been developed within the context of different environments and targeting different requirements.

In this research work, we present "**A policy and trust-based secure protocol"** that establish trust between interacting parties to share information easily and seamlessly across many different networks and databases, and make trusted partners capable of predicting the security risks and attacks in their communication systems. Accordingly, trust and policy–based certificates will be included in the proposed secure protocol so that the information sharing will be secure. This secure information sharing approach requires the following:

1. It requires public keys of the communicating parties such as customer, service provider, and government departments.

2. Session keys and secrete values are needed in this secure communication protocol to provide data privacy and integrity.

3. Trust factor of service provider is needed for government department. Based on the Service Provider's Trust Factor, Government Departments have to decide whether full or partial Client's information are to be sent to service provider from its database in a secured way.

The session keys and secretes values which play vital roles in secure communication procol, are generated from CBPRNG [10]. The communication parties can exchange their public keys, session keys and secrete values through secure communication protocol [3] without using trusted certificate authority (CA). Government departments obtain the trust factor of specified service provider by using reputation-based dynamic trust evaluation model [11].

This paper is structured as follows: the second section discusses the brief review of related works, and the third section presents our proposed policy, and trust based secure protocol, and the fourth section shows result of our proposed technique. Finally, the conclusions are summed up in fifth Section.

2. RELATED WORKS: A SHORT REVIEW

Literature presents a lot of works for secure communication in diverse applications. Here, we review some of the works presented in the literature.

Headayetullah, G.K. Pradhan [4] have recommended an efficient role and cooperation based information sharing approach for secure exchange of confidential and top secret data amongst security personals and government departments within the national boundaries using public key cryptography. The devised approach makes use of cryptographic hash function; public key cryptosystem and a unique and complex mapping function for securely exchanging confidential information. Furthermore, the approach facilitated privacy preserving information sharing with probable restrictions based on the rank of the security personals.

Muntaha Alawneh and Imad M. Abbadi [5] have suggested a mechanism that enables the source organization to send content based on organization policy and requirements to another collaborating organization in such a manner that it could be accessed only by a specific group of users performing a particular task or by all device members in the destination organization. They have consummate this by providing a hardware-based root of trust for the master controller and organization devices exploiting trusted computing technology.

Peiwu Li [7] has proposed a temporal model for Group-Centric Secure Information Sharing (g-SIS), which takes the temporal intervals of group and access enabling into consideration. They gave the temporal logic specifications of the model, and discussed a usage scenario to illustrate practical application in secure meeting system.

Peng Liu, Amit Chetal [8] have recommended an interest-based trust model and data sharing protocol, where a family of data sharing policies were integrated, and data exchange and trust negotiation were interleaved with and interdependent upon each other. In addition, an implementation of this protocol was presented using the emerging technology of XML Web Services. The implementation was totally compatible with the Federal Enterprise Architecture reference models and can be directly integrated into existing E-Government systems.

Ravi Sandhu *et al.* [9] have presented a framework (PEI) of three layered models to analyze requirements and develop solutions, and demonstrated the application of this framework in context of TC and secure information sharing. The three layers were policy models (topmost), enforcement models (middle), and implementation models (bottom). An essential benefit of PEI was that the three layers allowed us to focus on the more important issues at a higher level of abstraction at the policy and enforcement layers, while leaving deep detail to the implementation layer. They focused on the policy and enforcement layers with only passing mention of the implementation layer.

In [4] , [5], [7] ,[8], [9] they have used the trusted information sharing security protocols for the content sharing between collaborating organizations but they had not used a standard protocol for policy and trust-based information sharing. In this research work, we suggested the policy and trust based secure protocol for exchanging information between communicating parties more securely.

3. PROPOSED POLICY AND TRUST-BASED SECURE PROTOCOL

In this information age, Government information is a significant asset that must be held in trust and effectively managed by government. Government departments give more importance on the exchange of data and information between and among its trusted partners. With the capable information sharing solutions, trusted partners will be able to predicting the security risks and attacks on their information transfer. However, building secure information sharing mechanism between and among government and non-government

organizations is not trivial because they bother that their interest may be exposed when their information is shared with other organizations.

This section presents a policy and trust-based information sharing approach for secure exchange of confidential information between and among trusted partners such as service provider (private/public financial institutions), and government departments. Even though the proposed approach is non-privacy preserving, it assures great confidentiality and authentication, and trust between and amongst its trusted partners while transferring information. In general, the service provider obtains secrete information about customer from various government departments based on its trust factor. During the exchange, if information is hacked by some body, the service provider's further actions will go wrong. This demands an efficient and secure approach that offers confidential and authenticated information sharing without creating any issues and problems to security. Furthermore, there is a chance that government departments may provide complete confidential information about a customer to other service providers, which could affect the privacy of that customer and lead to information leakage. The above cases cannot be entirely avoided in a non-privacy-preserving approach but could be controlled by permitting information transfer based on the rate of trust factor of service provider.

In this suggested approach, the credibility of sharing information and providing service is based on service provider's trust factor and loan approval policy. Accordingly, trust and policy–based certificates will be included in the proposed secure protocol so that the information sharing will be secure. The proposed protocol provides greater data integrity, confidentiality by using private and public key cryptosystems, controlled privacy by predefined trust factor of service provider without creating any issues and problems to information security.

In this paper, we suggest "a policy and trust based secure protocol' for information sharing. In this paper, we use three nodes as customer, service provider and government departments. In this model Customer's information containing identity proof, income proof, residential proof etc., will be with Government Department. Service Providers, like Bankers etc., will give service to Customer on fulfillment of Service Provider's policy. When a customer requests for service, Service provider will contact with various Government Departments (such as income tax, revenue, insurance etc) for the requesting Customer's information. Then Government Departments will send the Customer's information from its database based on the Service Provider's Trust Factor in a secured way. If information is not available for the requested Customer from the Government Departments, then Service Provider will request the Customer to register information with the Government Departments. After receiving the customer details from the government departments, the service provider checks those details of the customer with its service approval policy to provide the service to the customer. If the customer details are not satisfied with the policy of the service provider, the service provider will not provide the service to the customer. Otherwise, the service provider will send 'service approval message to the customer. The steps involved in the proposed policy and trust based secure protocol are organized in the following sub sections:

3.1 Steps involved in proposed secure protocol at the customer

3.1.1. The construction of the customer's request message

The customer sends request message to service provider for getting its service. It is the duty of the customer to transmit its request to service provider in an unintelligible possibly encrypted manner such that hackers cannot extract any valuable information or alter the information in the request. Figure: 1 shows the steps involved in structuring the customer's request message.

Steps involved in *customer's* request message are:

1. A random number R_1 is chosen as request number and encrypted with customer's private key KR_c to obtain encrypted Random number E_{R1}. Later R_1 will be used to verify if the response corresponds to the appropriate customer's request.

$$\mathbf{E_{R1}=E[R_1]_{KRc}}$$

Where E denotes encryption.

2.After that encrypted Random number $E_{R1,}$ customer's personal identity C_{Pid} and customer's identity proof documents set $C_{proofdocs}$ are combined with the customer's query C_{query} to form the Customer 's data C_{Data}.

$$\mathbf{C_{Data}=E_{R1}+C_{Pid}+C_{proofdocs}+C_{query}}$$

Where C_{query} is the request query for getting service from service provider, and

$$C_{proof\ docs} = \{d_1, d_2, d_3, d_4, \ldots\ldots\ldots\}$$

Where d_1, d_2, d_3,d_4…….. are customer's proof identity documents

3. A secrete /Random value S_1 is chosen and combined with Customer's data C_{Data} , and then the result is hashed with SHA-1 to obtain hash H_1. The hash value is used to ensure that the customer request reaches the service provider untampered.

$$\mathbf{H_1=SHA\text{-}1\ [\ C_{Data}+S_1\ ]}$$

4. The hash value H_1 is added to Customer's data C_{Data}, and then the result can be encrypted with session key KS_1 to obtain customer's request message C_{MSG}.

$$\mathbf{C_{MSG}=E_{KS1}\ [H_1+C_{Data}\ ]}$$

The encryption with the session key reliably provides authentication and confidentiality to customer's request message C_{MSG}. Now, this structured customer request message C_{MSG} is transmitted to the service provider.

5. Session key $\mathbf{KS_1}$, customer public key **KUc**, and secrete value $\mathbf{S_1}$ **are** combined to obtain key message**,** and then it is sent to service provider through secure communication protocol [3].

$$\mathbf{Key_{MSG1}=S_1+KUc+KS_1}$$

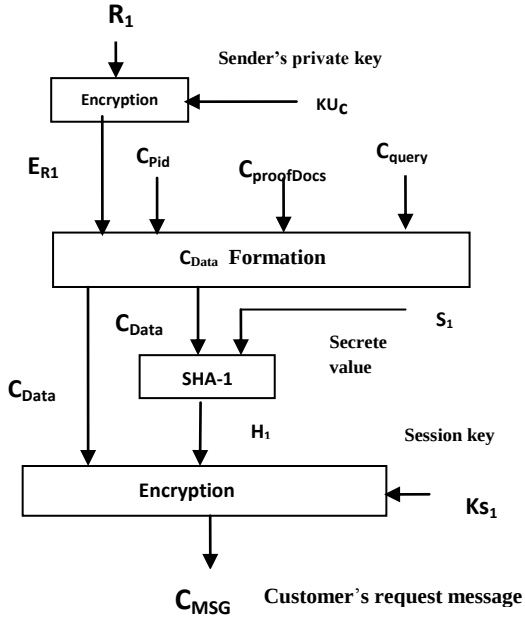


Figure 1: shows the steps involved in structuring the customer's request

3.2. Steps involved in proposed protocol at the Service Provider

3.2.1. Validation of the Customer's request message at SP

After receiving customer's request message $\mathbf{C_{MSG}}$ **and** key message $\mathbf{Key_{MSG1}}$, first SP decrypts key message $\mathbf{Key_{MSG1}}$ sent through secure communication protocol [3] to obtain **KUc**, secrete value S_1, and session key KS_1**.** Then, the SP must authenticate the customer followed by validating the integrity of the customer data. Figure: 2 shows the steps involved in validating the customer's request by SP.

The steps involved in validating the customer's request are as follows:

i) The request originated from the true or intended customer
ii) Integrity of the customer's request.

i). The customer's request message C_{MSG} , **which** contains encrypted customer data C_{Data} and hash value H_1 with session key KS_1 is as follows:

$$C_{MSG} = \mathbf{E}_{KS1}[H_1 + C_{Data}]$$

First C_{MSG} is decrypted with session key $\mathbf{KS_1}$ to obtain $\mathbf{C_{Data}}$ and hash value H_1. The successful decryption assures that confidentiality is added to the customer request message.

$$D_{KS1}[C_{MSG}] = C_{Data} + H_1$$

Where D denotes decryption and $\mathbf{C_{Data}} = \mathbf{E_{R1}} + \mathbf{C_{Pid}} + \mathbf{C_{proofdocs}} + \mathbf{C_{query}}$

After that E_{R1} is extracted from C_{Data}, and decrypted with customer's public key to obtain request number R_1. The successful decryption assures that the request has been authenticated and originated from claimed customer.

$$\mathbf{R_1 = D_{KUc}[E_{R1}]}$$

ii). For verifying the integrity of customer's data C_{Data} , SP possesses secrete value $\mathbf{S_1}$ and adds it to customer's data . Then, SP computes new hash value H_1^1 **over** concatenation customer's data C_{Data} and secretes value S_1. After that the SP compares H_1^1 with received hash value H_1. If the two matches, customer's request message is not tampered, otherwise, tampered.

$H_1^1 =$ **SHA-1 [** $\mathbf{C_{Data}}$ **+** $\mathbf{S_1}$**]**
IF $H_1 = H_1^1$ **then**
    $\mathbf{C_{Data}}$ **is not tampered**
ELSE
    $\mathbf{C_{Data}}$ **is tampered**
ENDIF

After evaluating all the parameters in the customer's request, the SP considers it as a valid request from the valid customer.

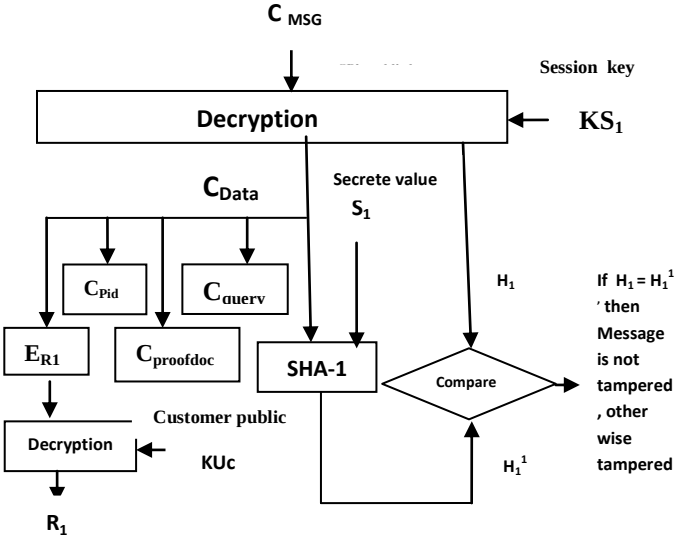


Figure 2: the validation of customer's request by service provider

3.2.2. The construction of the service provider request message

After validating customer's request $\mathbf{C_{MSG}}$, SP prepares the request message SP_{MSG} and sends it to GDs for sharing customer's information. It is the duty of the SP to transmit its request in an unintelligible possibly encrypted manner such that the hackers cannot extract any valuable information or alter the information in the request. The block diagram in Figure:3 shows the steps involved in structuring the SP's request message.

Steps involved in construction of SP's request message are:

1. A random number $\boldsymbol{R_2}$ is chosen as request number and encrypted with SP's private key KR**sp** to obtain $\mathbf{E_{R2}}$. Later $\mathbf{R_2}$ will be used to verify if the response corresponds to the appropriate SP's request.

$E_{R2} = E_{KRsp}[R_2]$,
Where E denotes encryption.

2. Then , SP request number E_{R2}, customer personal id C_{Pid} , and SP's query SP_{query} are combined with service provider registration identity , SP_{Rid} to form service provider data SP_{Data} .

$$\mathbf{SP_{Data} = E_{R2} + C_{Pid} + SP_{query} + SP_{Rid}}$$

Where $\mathbf{SP_{Rid}}$ **is** SP's registration -id and SP_{query} **is** a request for getting customer details from GD.

3. The SP's data SP_{data} is combined with secrete value $\mathbf{S_2}$, and then the result is hashed with SHA-1 to obtain H_2. Here SHA-1 algorithm is used to maintain the data integrity.

$$\mathbf{H_2 = SHA\text{-}1[\ SP_{Data} + S_2\ ]}$$

4. For message authentication, the hash value H_2 **is** added to SP's data $SP_{data,}$ and then the result can be encrypted with session key KS_2 to form SP's request message SP_{MSG}.

$$\mathbf{SP_{MSG} = E_{KS2}\ [\ H_2 + SP_{Data}\ ]}$$

The encryption with the session key reliably provides confidentiality to customer's request message C_{MSG}. Now, this structured SP request message SP_{MSG} is transmitted to GDs.

5. Session key $\mathbf{KS_2}$, SP's public key **KUsp**, and secrete value $\mathbf{S_2}$ **are** combined to obtain key message $\mathbf{Key_{MSG2}}$, and then it is sent to GDs through secure communication protocol [3].

$$\mathbf{Key_{MSG2} = S_2 + KUsp + KS_2}$$

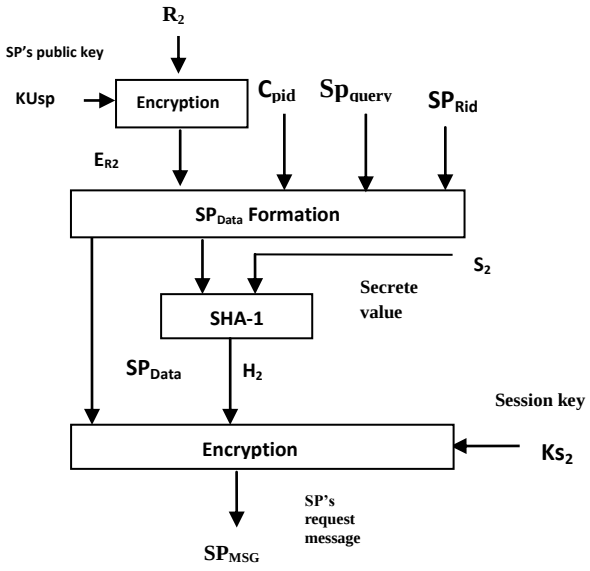


Figure 3: shows the steps involved in structuring the service provider's request

3.3. Steps involved in proposed protocol at various Government Departments(GDs)

After receiving service provider's request message $\mathbf{SP_{MSG,}}$ **and** key message $\mathbf{Key_{MSG2}}$, first GDs decrypt key message $\mathbf{Key_{MSG2}}$ sent through secure communication protocol [3] to obtain both secrete value S_2, **KUsp,** and session key $\mathbf{KS_2}$**.** Then, the GD must authenticate the SP followed by validating the integrity of the SP's request data.

3.3.1. Validation of the SP's request message at various GDs.

The steps involved in the above process are as follows:

i) The request originated from the true or intended SP

ii) Integrity of the SP's request.

i) The sp's request message SP_{MSG}, **which** contains encrypted SP_{Data} **and** H_2 with session key KS_2, is as follows:

$$\mathbf{SP_{MSG} = E_{KS2}\ [H_2 + SP_{Data}\ ]}$$

First, $\mathbf{SP_{MSG}}$ is decrypted with session key $\mathbf{KS_2}$ to obtain SP_{Data} and H_2. The successful decryption assures that confidentiality is added to SP's request message.

$$\mathbf{D_{KS2}[SP_{MSG}] = SP_{Data} + H_2}$$

Where D denotes decryption, and $\mathbf{SP_{Data} = E_{R2} + C_{Pid} + SP_{query} + SP_{Rid}}$.

After that $\mathbf{E_{R2}}$ is extracted from $\mathbf{SP_{Data}}$ and decrypted using SP's public key to obtain request number R_2. The successful decryption assures that the request has been authenticated and originated from claimed SP.

$$\mathbf{R_2 = D_{KUsp}\ [E_{R2}]}$$

ii. For verifying the integrity of SP's data SP_{Data}, GD adds S_2 to SP's data SP_{Data} and compute hash value H_2^1 **over** concatenation SP's data SP_{Data} and secrete value S_2. The GD compares H_2^1 with received hash H_2. If the two matches, request message is not tampered, otherwise tampered. Figure4 shows the steps involved in validating the SP's request data.

$$\mathbf{H_2^1 = SHA\text{-}1\ [\ SP_{Data} + S_2]}$$

IF $\mathbf{H_2 = H_2^1}$ **then**

$\mathbf{SP_{Data}}$ **is not tampered**

ELSE

$\mathbf{SP_{Data}}$ **is tampered**

ENDIF

After evaluating all the parameters in the SP's request, the GD considers it as a valid request from the valid SP.

3.3.2. The construction of the GDs's response message

The GDs send their response message to SP about the customer information. It is the duty of the GD to transmit the response in an unintelligible possibly encrypted manner such that the hackers cannot extract any valuable information or alter the information in the request. After validating the integrity of SP's request data, GD prepares the response message for SP's query based on its trust factor and sends it back to SP.

Trust factor

It is a value that checks the information of a certain organization by using organization-id and decides whether it is a reliable organization to share the information about a customer.

After receiving request from service provider to get particular customer details, each government department checks the service provider's registration-id SPR_{id} in its service provider's trust factor database. If SPR_{id} is not present in its government department database, the government department lets service provider to create its register-id. If the service provider's registration id SPR_{id} exists, then the corresponding government department would check the customer personal-id in its customer's details database to

share the customer details with the service provider. If Cp_{id} is not present in the database of the government department, it sends the information as wrong customer personal identity **Cp_{id}** to the service provider.

After checking the service provider's registration-id SPR_{id} and CP_{id} and if both exist, respective government departments check the trust factor of that service provider to share the limit of customer information with that the service provider. It is explained as

If TF $\geq$ 0.7
GDs will send full customer details to service provider
Else If TF $\geq$ 0.5
GDs will send limited customer details to service provider
Else GDs will send no customer details to service provider

Where TF is trust factor of service provider and its value must be in range from 0.0 to 1.0.

The above equation delineates that if the information in the database about the service provider has trust factor greater than or equal to 0.7, the government department would provide full details to the service provider about that customer. If the rate is greater or equal to 0.5, the government department would provide limited details about the customer to the service provider. Otherwise, GDs will not send customer details to service provider

Steps involved in GD's response message are:

1. A random number ***R_2 [1] received from SP*** is chosen as response number and encrypted with GD's private key KR_{GD} to obtain $\mathbf{E_{R2}}$.

$\mathbf{E_{R2}=E_{KRsp}\ [R_2^1]}$ **Where** E denotes encryption.

2.After that , $\mathbf{E_{R2}^1}$, customer details $C_{\textbf{customer details}}$ based on SP's trust factor, and GD identity GD_{id} are combined to form government department response data $GD_{ResData}$.

$\mathbf{GD_{ResData}= C_{customer\ details} + E_{R2}^1 + GD_{id}}$

Where $C_{customer\ details}$ is details of the intended customer.

3. Then GD's response data $\mathbf{GD_{ResData}}$ is combined with secrete value S_3 and then hashed with SHA-1 to obtain H_3.

$$\mathbf{H_3=SHA\text{-}1[GD_{ResData} + S_3]}$$

4. The hash value H_3 and response message $\mathbf{GD_{resdata}}$ are combined, and then the result can be encrypted with session key KS_3 to form GD's response GD_{RESMSG}.

$$\mathbf{GD_{RESMSG} = E_{KS3}\ [H_3 + GD_{ResData}]}$$

The encryption with the public key reliably provides confidentiality. Now, this structured GD response message $\mathbf{GD_{RESMSG}}$ is sent to the SP. Figure 4 shows the steps involved in structuring the GD's response.

5. Session key $\mathbf{KS_3}$, GD's public key $\mathbf{KU_{GD}}$ and secrete value $\mathbf{S_3}$ **are** combined to obtain key data $\mathbf{Key_{MSG3}}$, and then it is sent to SP through secure communication protocol [3].

$$\mathbf{Key_{MSG3} = S_3 + KU_{GD} + KS_3}$$

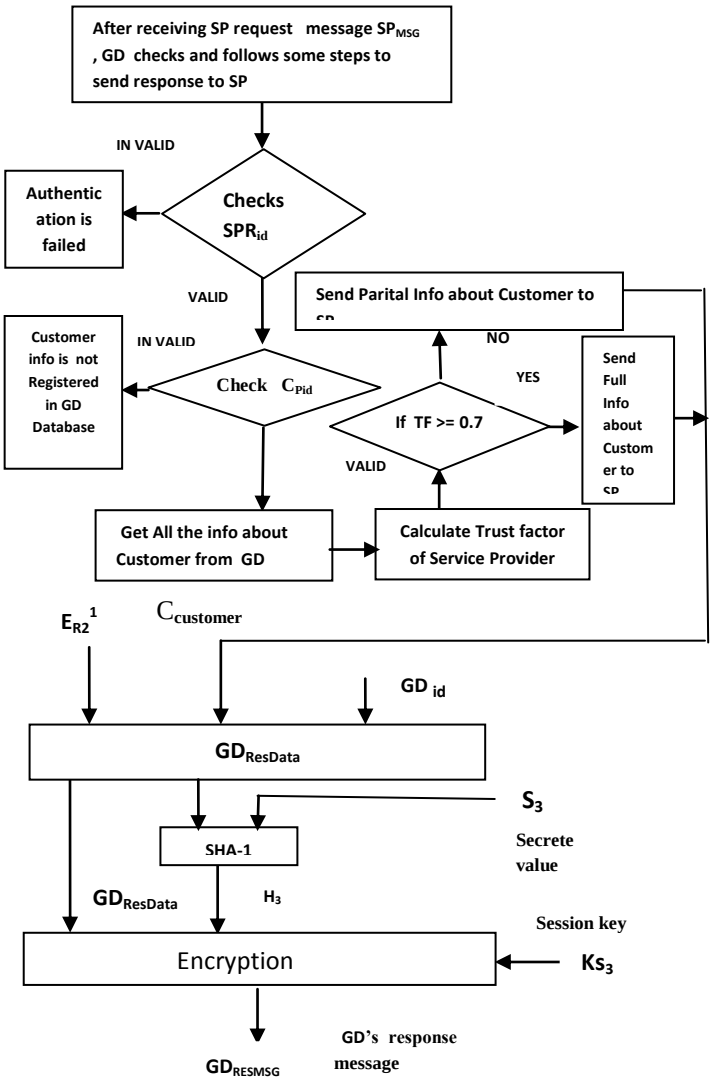


Figure 4: Explains checking the trust factor of SP and customer personal-id C_{Pid}, and prepares structuring of GD's response message to SP.

3.4. Steps involved in proposed protocol for GDs's response message at SP

After receiving GDs's response GD_{RESMSG} **and** $_{key}$ message $\mathbf{Key_{MSG3}}$, first SP decrypts key message $\mathbf{Key_{MSG3}}$ sent through secure communication protocol [3] **to obtain S_3 , KU_{GD} and KS_3.** Then, SP must authenticate the GD followed by validating the integrity of the GD's response data.

3.4.1. Validation of GD's Response message at SP

The steps involved in the above process are as follows**:**

i) he response originated from the true or intended GD
ii) Integrity of the GD's response
iii) The response corresponds to the opt request of the SP.

i. The GD's response message GD_{RESMSG}, which contains encrypted $GD_{ResData}$ and H_3, is as follows.

$$\mathbf{GD_{RESMSG}= E_{KS3}\ [GD_{ResData} + H_3\ ]}$$

First, $\mathbf{GD_{RESMSG}}$ is decrypted with session key $\mathbf{KS_3}$ **obtained from GD** to obtain $\mathbf{GD_{ResData}}$ and H_3.

$$\mathbf{D_{KS3}\ [GD_{RESMSG}\ ] = GD_{ResData} + H_3}$$

Where D denotes decryption and $\mathbf{GD_{ResData}= E_{R2}^1 + C_{customer\ details} + GD_{id}}$

This successful decryption assures that the received message provides confidentiality.

After that $\mathbf{E_{R2}1}$ is extracted from $GD_{ResData,}$ **and** then decrypted with GD's public key to obtain response number $R_2{}^1$. The successful decryptions assure that $GD_{ResData}$ has been originated from claimed GD.

$$\mathbf{R_2{}^1=D[E_{R2}{}^1]\ KU_{GD}}$$

ii. The response is confirmed for its integrity by computing new the hash value $H_4{}^1$and comparing it with the hash value H_4 received from GD. If the two matches, the response is not tampered, otherwise tampered.

$$H_3 = SHA\text{-}1\ [\ GD_{ResData}\ + S_3\ ]$$
$$IF\ H_3 == H_3{}^1\ then$$
Information is not tampered
ENDIF

iii. If the obtained response number $\mathbf{R_2{}^1}$ is same as the SP's request number $\mathbf{R_2}$, it makes sure that the response is valid for the request made. The successful decryption assures that the *response has been originated from* the true or intended GD.

$$IFR_2 = R_2{}^1$$
The response is valid
ENDIF

After evaluating all the parameters in the GD's response, the SP considers it as valid response from the valid GDs.

3.4.1 The construction of the SP's response message

After validating the GD response GD_{RESMSG}, SP prepares and sends the response message for appropriate customer's request based upon its service approval policies. . Figure:5 shows then steps involved in structure of the SP's response

In this paper, we suggest two types of security policies: information security and organization's policies.

Information security policies are services that provide security for data that transferring from source system to destination system. We consider some these policies such as *authentication, confidentiality, data integrity, non–repudiation and availability* that may need to be met in communication networks.

Organization's policies ***are*** the terms of certain organization that should abide by the customers to get the benefit from that organization. These are generally adopted by Board of governance body within an organization where procedures or protocols would be developed and adopted by senior executive officers. *In* this paper, Service provider addresses organization policies that constraints on its members who need service. After receiving the encrypted customer details from the corresponding government departments, the service provider decrypts the customer details and checks it with its policy. The policy may contain the terms such as rules and regulations prescribed by central bank (for example RBI (Reserve Bank of India)), the nativity of the customer must be within a certain region, the customer's date of birth should be within a certain limit, the assets of the customer should be greater than certain limit, Credit score must be within the limit etc. A credit score is individual detailed credit history and full evidence of customer worthiness. Based on customer credit history, CIBIL gives customer score between 300 and 900 to service provider. The higher individual score the greater are his chances of service approval.

The construction *of* the SP's response involves the following steps:

1. A random number R_1 *received from customer is* chosen as response number $\boldsymbol{R_1{}^1}$, ***and*** then encrypted with SP's private key KR_{SP} to obtain $\mathbf{E_{R1}{}^1}$. Later $\boldsymbol{R_1{}^1}$ will be used to verify if the response corresponds to the appropriate SP's request.

$E_R{}^1=E_{KRsp}[R_1{}^1]$, where E denotes encryption.

2.After that , the SP prepares response message which includes encrypted response number $\mathbf{E_{R1}}$, and SP 's response $\mathbf{SP_{Response}}$ based on SP's policy and its identity SP_{id} to form service provider response data $SP_{ResData}$

.

. $\mathbf{SP_{ResData}= SP_{Response} +E_{R2}+ SP_{Rid}}$ Where $SP_{Response}$ is SP's response message to customer request.

3. SP's response data $\mathbf{SP_{ResData}}$ is combined with secrete value S_4, and hashed with SHA-1 to obtain H_4.

$$\mathbf{H_4 = SHA\text{-}1[\ SP_{ResData}\ + S_4\ ]}$$

4. The hash value H_4 and response message $SP_{Resdata}$ are combined, and then the result can be encrypted with session key KS_4 to form SP's response message SP_{RESMSG} .

$$SP_{RESMSG} = \mathbf{E_{KS4}\ [\ H_4\ +\ SP_{ResData}\ ]}$$

The encryption with the public key reliably provides confidentiality. Now, this structured response SP_{RESMSG} is sent back to the customer

5. Session key $\mathbf{KS_4}$, SP's public key **KUsp**,and secrete value $\mathbf{S_4}$ **are** combined to obtain key message $\mathbf{Key_{MSG4}}$, and then it is sent to customer through secure communication protocol [3]

. $$\mathbf{Key_{MSG4} = S_4 + KUsp + KS_4}$$

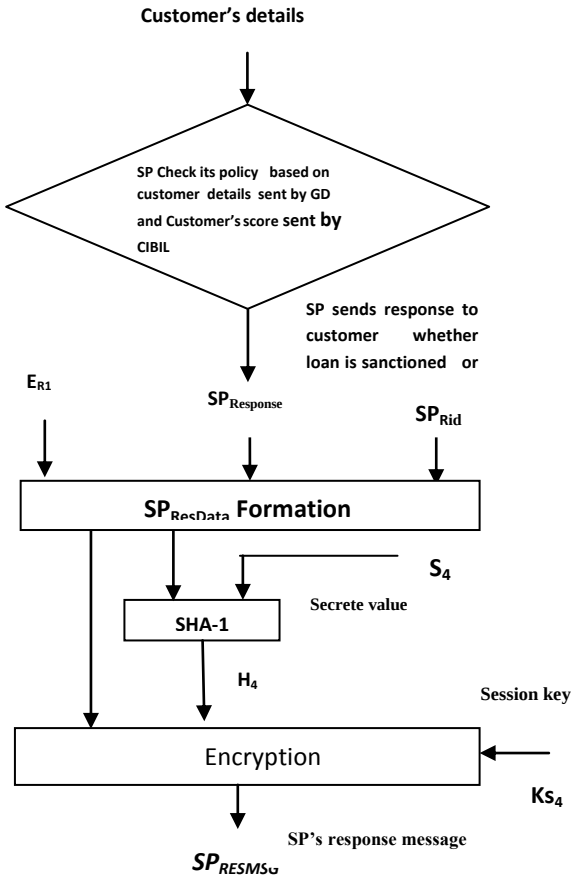


Figure 5 shows the steps involved in structure of the SP's response

3.4 The Steps involved in proposed protocol for the SP's response at customer

After receiving SP's response SP_{RESMSG} **and** key data Key_{MSG4}, first customer decrypts key data Key_{MSG4} sent through secure communication protocol [3] **to obtain S_4, KUsp and KS_4.** After that, the customer must authenticate the SP followed by validating the integrity of the SP's response data.

3.5.1 Validation of service provider's Response at the customer.

After receiving the response from the SP, the customer must ensure the following:

i) The response originated from the true or intended SP

ii) Integrity of the SP's response

iii) The response corresponds to the opt request of the customer.

i. The received response $SP_{RMSG,}$ which consists of encrypted $SP_{ResData}$ and H_4 with session key $\mathbf{KS_4}$, is follows:

$$SP_{RESMSG} = E_{KS4} [\ H_4 + SP_{ResData}\ ]$$

First SP_{RESMSG} is decrypted with session key $\mathbf{KS_4}$ to obtain $\mathbf{SPA_{ResData}}$ and hash value H_4.

$$\mathbf{D [\ SP_{RESMSG}\ ]_{KRsp} = SP_{ResData} + H_4}$$

Where $\mathbf{SP_{ResData} = SP_{Response} + E_{R1}^{1} + SP_{Rid}}$

The successful decryption assures that authentication and confidentiality is provided to the SP's response message.
The $\mathbf{E_{R1}^{1}}$ is decrypted with SP public key $\mathbf{KU_{SP}}$ to obtain SP's response number R_1^1. The successful decryptions assure that $\mathbf{SP_{ResData}}$ is an originated from SP.

$$\mathbf{R_1^1 = D[E_{R1}^{1}]\ KU_{SP}}$$

ii. The response is confirmed for its integrity by computing new the hash value $H_4^1$and comparing it with the hash value H_4 received from SP. If the two matches, the response is not tampered, otherwise tampered.

***H4= SHA-1*[$\mathbf{SP_{ResData}}$, $\mathbf{S_4}$]**
***If* $H_4 == \mathbf{H_4^1}$**
Information is not tampered
Endif

iii. If the obtained SP's response number $\mathbf{R_1^1}$ is same as the customer's request number $\mathbf{R_1}$, it makes sure that the response is valid for the request made.

IF $R_1 = R_1^1$
The response is valid
ENDIF

After evaluating all the parameters in the SP's response, the customer considers it as a valid response from the valid SP.
All above steps ensures that the proposed policy and trust based secure protocol is effective in providing authentication, data integrity, confidentiality and secure information sharing.

Figure:6 shows the steps involved in the validation of SP's response.

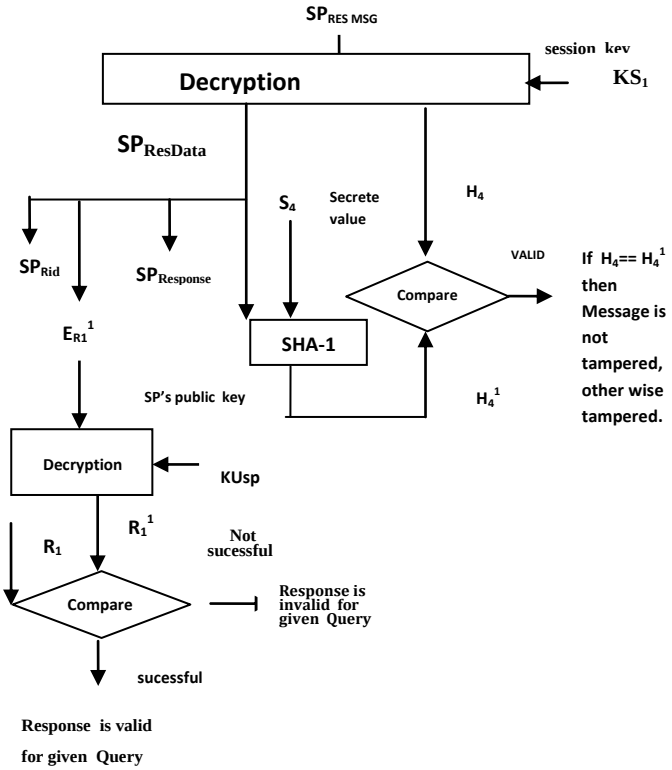


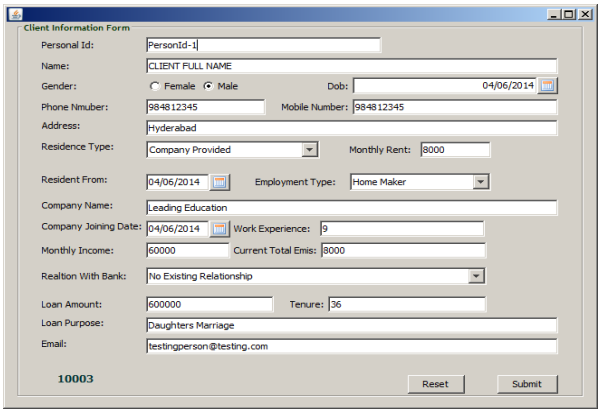
Figure 6: the validation of service provider's response by customer

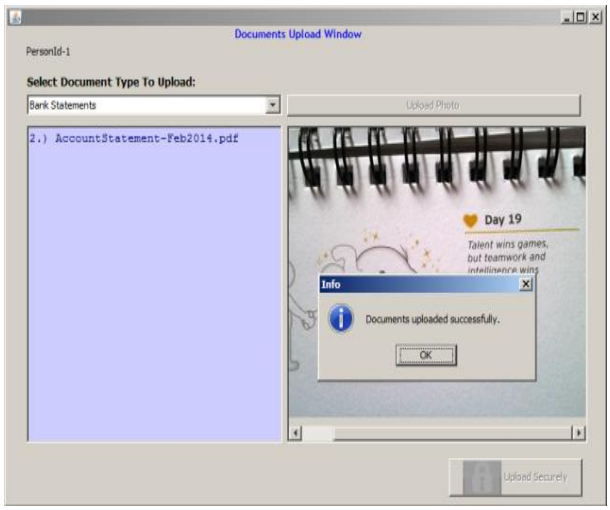
4. RESULT AND DISCUSSION

This section details the information we used to structure the database of the government departments for checking the trust factor of the service provider and for checking the details of the customer and the results we obtained for our proposed policy and trust based information sharing using that data base. Our experimentation done in the system which has Intel Core2 Duo processor with 2.93 GHZ clock speed, Windows 7 Operating System and 2 GB RAM. Our technique was implemented in Java (jdk 1.6) and the editor which we used is Net Beans IDE 7.4.

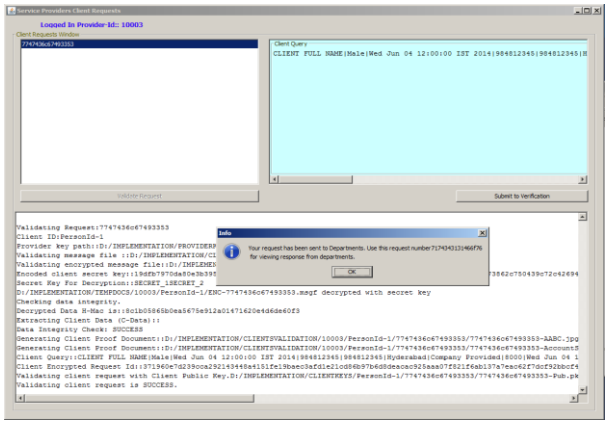
In this section, we have presented the experimental results of the policy and trust based secure communication protocol used in information systems. The results obtained from experiments illustrates that the presented protocol is effective secure information sharing among customer, service provider and government departments. First, process started with a customer request for getting service from service provider. After validation of the customer request, the service provider sends request to government department for sharing confidential information about specified customer. After validation of SP's request, the government departments respond to service provider with the subset of customer information based on the trust factor of service provider. After validating the legitimacy and authentication and confidentiality of the appropriate governments responses, service provider check its service approval policy with customer information sent from various government departments. After that, service provider takes decision whether to provide service to the customer or not.

Screen 1: Customer selects a service provider and submits his/her details along with proof documents through a secured communication channel.

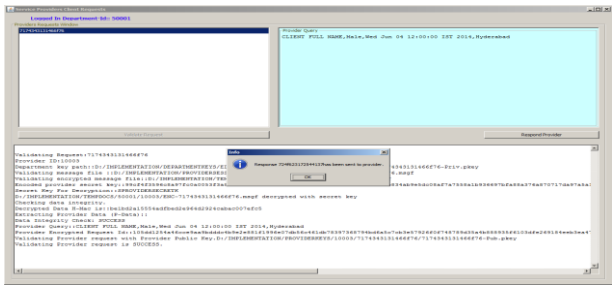




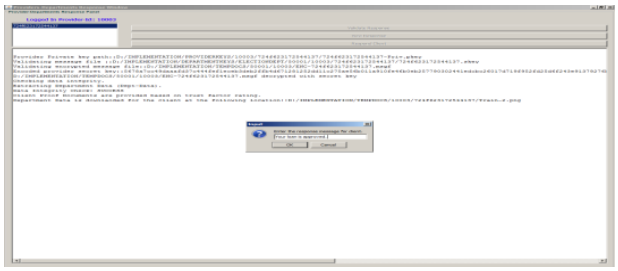
Screen 2: Service provider views customer requests, validates the request, and enquires with government departments against the submitted proof documents.



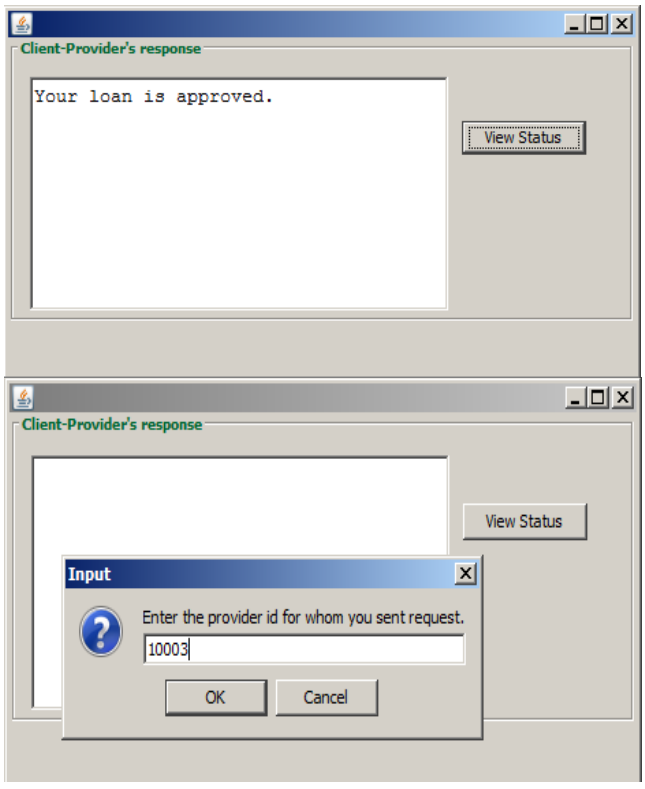
Screen 3: Government Departments, validates the provider request and searches for the customer information as provided by the service provider, if customer information is available it will be shared to service provider based on the service provider trust factor rating.



Screen 4: Provider validates Government Department response and verifies the customer proof information against the customer submitted proof information. Based on Service Provider's policy SP responds to customer request and informs him/her whether they can provide service or not.



Screen 5: Customer checks the request status submitted to a service provider.



5. CONCLUSION AND FUTURE RESEARCH

In the proposed approach, the credibility of customer's information shared from government departments to service provider is based on the trust factor of service provider. Our proposed policy and trust-based secure communication protocol approach can avoid problems of more necessitate information sharing, coordination and collaboration amongst government and non -government organizations within a country and across national boundaries. The proposed secure information sharing approach has offered several security issues such as confidentiality, authentication, integrity, and non-repudiation with help of cryptographic hash algorithm, private and public cryptography. Also, on the basis of a predefined trust factor of service provider, a restricted privacy is maintained between the service provider and government departments. The effectiveness of the proposed approach has been demonstrated with help of experimental results. The proposed approach could preferably use in cloud computing during the exchange of documents or services. Parties who are exchanging their documents or services may take trust factors into account to have trustworthy relations. We propose some future trust models such as trusted medical applications, trusted storage services, trusted email customers.

6. REFERENCES

[1] Hui-Feng Shih and Chang-Tsun Li, "Information Security Management in Digital Government", Vol. 3, pp. 1054 - 1057, Idea Group Publishing, 2006.

[2] Violetta Cavalli-Sforza, Jaime G. Carbonell and Peter J. Jansen , "Developing Language Resources for a Transnational Digital Government System", Language Technologies Institute, Carnegie Mellon University ,Pittsburgh, U.S.A, 2004.

[3] T.Chalama Reddy and R.Seshadri, "Design of new protocol for secure communication of Messages", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[4] Md. Headayetullah, G.K. Pradhan , " Efficient and Secure Information Sharing For Security Personnels: A Role and Cooperation Based Approach ", International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010, 1254-1265.

[5] Muntaha Alawneh, Imad M. Abbadi, "Preventing information leakage between collaborating organisations", Proceedings of the 10th international conference on Electronic commerce, Innsbruck, Austria, Article No.: 38, 2008.

[6] Achille Fokoue, Mudhakar Srivatsa, Pankaj Rohatgi, Peter Wrobel, John Yesberg, "A decision support system for secure information sharing", Proceedings of the 14th ACM symposium on Access control models and technologies, pp:105-114, 2009.

[7] Peiwu Li, "A Temporal Model for Group-Centric Secure Information Sharing", Web Information Systems and Mining (WISM), 2010 International Conference on, pp. 59- 62 , 2010.

[8] Peng Liu, Amit Chetal, "Trust-Based Secure Information Sharing Between Federal Government Agencies", Journal Of The American Society For Information Science And Technology—February 1, 2005.

[9] Ravi Sandhu, Kumar Ranganathan and Xinwen Zhang, " Secure Information Sharing Enabled by Trusted Computing and PEI Models", ASIACCS '06 March 21-24, 2006, Taipei, Taiwan.

[10] T.Chalama Reddy , Dr.R.Seshadri, " New Design of Crypto-Based Pseudorandom number generator (CBPRNG)using BLOW FISH cipher" International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 5 No. 06 Jun 2013 pages 561-566

[11]. T.Chalama Reddy , Dr.R.Seshadri, "Reputation-Based Dynamic Trust Evaluation Model for multi-agent Systems based on service satisfaction" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250–2459, Volume 4, Issue 6, June 2014)

[12] Kartheesn L, S.K Srivatsa, "A Policy Based Scheme for Combined Data Security in Mobile Ad hoc Networks" Journal of Computer Science 8(8): 1397-1406, 2012