Efficient and Secure Information Sharing For Security Personnels: A Role and Cooperation Based Approach

Md.Headayetullah
Assistant Professor, Department of CSE/IT
Dr.B.C Roy Engineering College
Duragpur-713206
West Bengal University of Technology (WBUT)
West Bengal, India
PhD Scholar, SOAU
E-mail: headayetullahphd1@gmail.com

G.K. Pradhan
Professor and Head
Department of CSE/IT,
ITER, SOA University Bhubaneswar
Ph.D (IIT Kanpur)
India
E-mail: gopa_pradhan@yahoo.com

***Abstract*—To facilitate users to interact with and share information without difficulty and faultlessly across various networks and databases nationwide, a secure and trusted information-sharing environment has been recognized as an imperative requirement and to advance homeland security effort. The key incentive following this research is to build a secure and trusted information-sharing approach for government departments. This paper presents an efficient role and cooperation based information sharing approach for secure exchange of confidential and top secret information amongst security personnels 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 proposed approach facilitates privacy preserving information sharing with probable restrictions based on the rank of the security personnels. The developed role and cooperation based information sharing approach ensures secure and stream-lined information sharing among security personnels and government intelligence departments to avoid threatening activities. The experimental results demonstrate the effectiveness of the proposed information sharing approach.**

Keywords-Digital Government, Government Intelligence Departments, Security Personnels, Information Sharing, Security, Mapping Function, Message Digest 5 (MD5), Public-Key Cryptosystem, Role, Cooperation, Rank.

I. INTRODUCTION

Government is a user of information technologies, contributor of information based services and major collector and supplier of data and information [1]. Globally, today many governments face challenges during traditional way of transformation and thus necessitate re-inventing the government systems so as to bring out efficient and cost effective services, information and knowledge via communication technologies [2]. A key step in reinventing government is through fostering digital government, which is nothing but the usage of widespread applications of information and communication technology that handles every transaction of government services [3]. Digital government is classically termed as the formation and transmittal of information and services within government and among government and the public by means of a range of information and communication technologies. The impact of digital government varies extensively across the world and is also known as e-government or virtual government [4]. E-government services are established in a complex architectural and technological scenario [5]. Information Age technologies afford huge opportunities for a government to transform its functions into the digital arena [6]. Many government agencies have insistently employed information technologies for updating the government's extremely fragmented service-centric information infrastructure by increasing information flow and the decision-making processes [6].

Information is an important aspect of government's resources. Therefore, at present, an urgent need to persuade and endorse larger flow of information is in demand along with data sharing between public agencies [7], [8]. The exclusive revolution in information resulted on organizations within the entire world to greatly rely upon huge numbers of databases to carry out their daily trade [9]. "Sharing information" is termed as the collection and sharing of intelligence between two security divisions, or sharing original e-crime data, observations on these data, surveillance notes, scientific facts, commercial transaction data, and other. Information differs in the level of detail, the quantity or type of data exchanged. Due to lack of standard methods for e-government information sharing, the means of sharing, at present are not uniformly monitored, authenticated and recorded [10]. The information sharing environment is intricate and innovative resolutions and partnerships are essential to collect shared benefits [11]. In addition, the sharing is not constantly assured to be harmless from risks that might embrace unauthorized access, malicious alteration, and destruction of information or misinformation, computer intrusions, copyright infringement, privacy violations, human rights violations and more [10]. Because government departments are in need to share information within the same government and also across governments, the devising of an effective security measure is essential. Still, a department cannot arbitrarily reveal its database to any another departments [25, 27].

A protected and trusted information-sharing environment is a requirement to enable users to converse with and share information without difficulty and flawlessly across a lot of dissimilar networks and databases nationwide. This means can considerably advance the efficacy of numerous functions, such as intelligence gathering and public safety efforts [22, 26, 28, 18]. Guarantying security for its information systems, together with computers and networks, is a basic necessity for a digital government to function to the hope of its people. Information security is nothing but protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The key elements of information security comprise integrity, confidentiality, availability, authentication that has to be considered at various levels inside the hierarchy [23]. Production of a wide basement for information sharing needs trust among all information sharing partners. Deficiency of trust leads to fears, that shared information will not be safeguarded frequently or used properly; and, that sharing will not constantly happen in both directions [24]. By using a secure information sharing system, organizations can participate with assurance in communities of trust since for this reason they have the controls so as to precisely govern their information accessing and usage.

Let us consider a local law enforcement officer at a standard traffic stop. Fundamental protocol utters that the officer request and confirm the individual's driving license and vehicle registration. Still, the officer might in addition check a broad range of other computer applications, such as immigration databases, terrorist watch lists, criminal information and intelligence repositories, and counter-drug intelligence databases that may be owned by external organizations, such as the U.S. Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Homeland Security. To perform this, these outwardly owned applications have to be capable to identify the officer so as to decide if he or she has the exact credentials to get the information. Afterward, the information that is liable to be sensitive from an intelligence and privacy perspective is ought to be protected while in transit. Lastly, the device on which the officer collects the information should be capable of storing that information securely [12]. In our earlier works, we have proposed efficient and secure information sharing protocols for secure exchange of confidential information amongst government intelligence agencies [29, 30].

In this paper, we present an efficient and secure information sharing approach for security personnels to share confidential information among them and with Government departments which deal with security. The proposed approach is principally tailored to fit in the following scenario. Consider, for example, a local law enforcement officer at a standard traffic stop. The standard protocol for traffic control necessitates the officer to request and verify the individual's driving license and vehicle registration. Nevertheless, the law enforcement officer could also wish to check with an extensive range of other computer applications, such as immigration databases, criminal information and intelligence repositories, and counter-drug intelligence databases that may be owned by external organizations, such as Central Bureau of Investigation (CBI), the Drug Enforcement Administration, and the Department of Homeland Security. The precision and the amount of information shared between security personnel and communicating government intelligence departments is based on the predefined rank of the security personnels. The proposed role and cooperation based information sharing approach achieves data integrity using a cryptographic hash function, MD5 Algorithm; confidentiality and authentication using Public Key Infrastructure (PKI) and department verification using a unique and complex mapping function.

The basic outline of the paper is as follows: A concise review of some recent researches related to the proposed approach is given in Section II. The proposed role and cooperation based information sharing approach for security personals is presented in Section III. The experimental results are presented in Section IV. Finally, the conclusions are summed up in Section V.

II. Review Of Related Research

Numerous researchers have presented approaches for secure and effective information sharing between communicating parties. Among them, a few researchers have presented approaches for securely sharing confidential information among government departments. In recent times, developing efficient approaches for securely sharing confidential information among government agencies and departments has drawn much attention. A concise review of some recent researches is presented here.

To address the information sharing issue amid government agencies, Peng Liu *et al.* [13] have presented an inventive interest-based trust model and an information sharing protocol, in which is included a group of information sharing policies also information exchange and trust negotiation are interleaved and mutually dependent on each other. Furthermore, the emerging technology of XML Web Services was utilized during the implementation of the proposed protocol. The implementation was completely consistent with the Federal Enterprise Architecture reference models and can be explicitly incorporated within current E-Government systems.

Jing F. *et al.* [15] have projected a theoretical model for information sharing in an e-government infrastructure. They ascertained that the Government-Government (G2G) information sharing model will help in giving knowledge for G2G information sharing and help decision makers in formulating decisions regarding the participation in G2G information sharing. The proposed conceptual model was checked to find out the aspects influencing the participation in an e-government information sharing and highlight the conceptual model via case study beneath Chinese government system.

Fillia Makedon *et al.* [14] have presented a negotiation-based sharing system called SCENS: Secure Content Exchange Negotiation System which was being constructed at Dartmouth College with the assistance of numerous interdisciplinary experts. SCENS was a multilayer scalable system that guarantees transaction safety via a number of security mechanisms. It was based on the metadata description of heterogeneous information which is applicable to various different domains. They represented that with sensitive and distributed information the government users can achieve settlement on the conditions of sharing through negotiation.

Xin L. [16] have established a distributed information sharing model as well as investigated the technique standard support of the model. It was deduced that the expenditure of dealing with government information exchange and cooperation between agencies will be minimized by a raise in the potential and efficiency of agencies' collaboration due to the secure e-government information sharing elucidations.

Nabil R. Adam *et al.* [17] have examined the demands in integration, aggregation and secure sharing information to facilitate situation consciousness and response at the strategic level. On extraction of data from various independent systems, the system filters, integrates, and proficiently envisages information indispensable to obtain a general operational picture, by utilizing context-sensitive parameters. One considerable demand was to assist secure information sharing. Sharing of information prolongs to be a major complexity due to the data privacy and ownership concerns as well as owing to a widespread range of security policies followed inside various government agencies.

Nabil Adam *et al.* [18] have presented a two tier RBAC approach to facilitate security and discriminative information sharing amid virtual multi-agency response team (VMART) as well as when there is need, it allows VMART expansion by permitting new collaborators (government agencies or NGOs). They also offered a coordinator Web Service for every member agency. The coordinator Web Service captures the responsibilities such as, authentication, information dissemination, information acquisition, role creation and enforcement of predefined access control policies. Realization of Secure, selective and fine-grained information sharing was accomplished by the encryption of XML documents in par with corresponding XML schema defined RBAC policies.

Achille Fokoue *et al.* [19] have founded logic for risk optimized information sharing through rich security metadata and semantic knowledge-base that detains domain specific concepts and relationships. They confirmed that the method was: (i) flexible: e.g., tactical information decomposing sensitivity in agreement with space, time and external events, (ii) situation-aware: e.g., encodes need-to-know based access control policies, and further outstandingly (iii) supports elucidations for non-shareability; these elucidations along with rich security metadata and domain ontology allows a sender to intelligently execute transformation of information with the intention of sharing the transformed information with the recipient. In addition, they have explained a secure information sharing architecture with the help of a commonly accessible hybrid semantic reasoner as well as showed a number of descriptive cases that highlights the benefits of the method while contrasting with conventional methodologies.

Ravi Sandhu *et al.* [20] have presented a way to share secure information easily through modern Trusted Computing (TC) technologies which is not available with pre-TC technology. They have configured the PEI framework of policy, enforcement and implementation models, and demonstrated its applicability in inspecting the issue and generating solutions for it. The framework enables the deep investigation of potential TC applications for secure information sharing in the upcoming work. TC applications excluding information sharing as well are expected to be scrutinized.

A group of policy-based technologies to provide augmented information sharing among government agencies without declining information security or person`s privacy has been developed by Tryg Ager *et al.* [21]. The method covers: (1) fine-grained access controls which support deny and filter semantics for fulfillment of complex policy conditions; (2) a oppressive policy ability that facilitates combination of information from various resources conforming to each source’s original disclosure policies; (3) a curation organization which permits agencies to use and scheme item-level security categorizations and disclosure policies; (4) an auditing system which deals with the curation history of every information item; and (5) a provenance auditing method that tracks derivations of information in excess of time to offer support in assessments of information quality. The final aspiration was to facilitate a capacity to resolve astonishing information sharing issues in government agencies and proffer ways for the growth of future government information systems.

Gail-Joon Ahn *et al.* [31] have dealt with the problem of supporting selective information sharing while reducing the possibility of unauthorized access. They have proposed system architecture by integrating a role-based delegation framework. In addition by implementing a proof-of-concept, they have verified the practicability of their framework.

Mudhakar Srivatsa *et al.* [32] have offered a calculus approach for secure sharing of tactical information. Three operators: Γ, + and · are supported by the security metadata which they have modeled as a vector half-space (as against a lattice in a MLS-like approach). A metadata vector is mapped into a time sensitive scalar value by the value operator Γ. On the metadata vector space that are homomorphic, arithmetic is supported by the + and · operators with the semantics of information transforms. In order to quantify the tightness of values estimates in the approach, they have built up concrete realizations of their metadata calculus that solves weak homomorphism without getting affected by metadata expansion utilizing B-splines (a class of compact parametric curves).

Muntaha Alawneh and Imad M. Abbadi [33] have presented 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 a specific group of users performing a specific task or by all device members in the destination organization. They have accomplished this by providing a hardware-based root of trust for the master controller and organization devices utilizing trusted computing technology.

III. Role And Cooperation Based Secure Information Sharing Approach For Security Personnels

Governments must keep in trust the critical asset, government information and manage it effectively. A greater priority must be given by government organizations at all levels for the exchange of information and data between and amidst its trusted partners. Information must be leveraged and assisted by coordinated and integrated solutions so as to meet the increasing needs and service requirements. The current "stove piped" environment has hindered the information sharing or exchanges among the agencies, the central government and the local jurisdictions. The lack of common data vocabularies for government intelligence departments has made information sharing with them both costly and complicated. Despite the fact that some improvement has been made, to specify how information sharing responsibilities and relationships, including proper central incentives will advance this task, more endeavors are needed [6]. Building secure information sharing mechanisms for security personnels is not trivial because security personnels worry that their interests may be jeopardized when they share information with government departments that are dealing with security [22]. The primary motivation behind this research is the design of an efficient and secure information sharing approach for securely exchanging confidential and top secret information among security personnels and government intelligence departments.

This section describes the role and cooperation based information sharing approach proposed for secure exchange of secret information among security personnels and government intelligence agencies. Although the proposed approach is non privacy-preserving, it assures paramount confidentiality and authentication in information transfer for both the security personnel and the target government departments. In general, the security personnels obtain secret information about suspicious persons and their activities from the government intelligence agencies. During the exchange, if the information is hacked by somebody, the security personnel's further actions will go wrong, which leads to a critical issue. 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 the target government department may provide complete confidential information about a person to all the security personnels, which would affect the privacy of that person and leads to information leakage. The above case cannot be entirely averted in a non privacy-preserving approach but could be controlled by permitting information transfer based on the security personnel's rank.

In the presented approach, the credibility of information shared is based on the rank of the security personnel. A master control is introduced in the proposed approach to monitor and control the information exchange between the security personnel and the government intelligence departments. The proposed secure information sharing approach requires the following: a) The public key of the security personnel, the master control and the communicating departments b) A unique and complex mapping function to uniquely identify the security personnels, the master control and the communicating intelligence department. The security personnels, the master control and the communicating government intelligence departments attain their public and private keys from a trusted Certificate Authority (CA). The major steps involved in the proposed information sharing approach are presented in the following sub-sections.

A. *Steps in the proposed approach at the security personnel side*

1) Structuring of the security personnel's query

The security personnel sends request for some secret information about susceptible persons and their suspicious activities to the government intelligence departments. It is the duty of the security personnel to transmit the request in an unintelligible possibly encrypted manner such that the hackers cannot extract any valuable information or alter the information in the request. The structuring of the security personnel's request involves the following steps:

1. A random number RV is elected and encrypted using the security personnel's public key K_S^{Pub}. This encrypted random number E_{RV} will be used to verify if the response corresponds to the apt security personnel's request.

$$E_{RV} = Enc[RV]_{k_S^{Pub}}$$

2. After that, a set of random values R are chosen and they are combined with the encrypted random number E_{RV} and the request to obtain the SE_{Data}. The random values set R will be utilized in the validation of the identity of the target government department.

$$R = \{r_1, r_2, r_3, \cdots, r_n\}$$
$$SE_{Data} = [E_{RV} + R + Query]$$

3. With the help of the MD5 Algorithm, the hash value H_v is computed from the SE_{Data}.

$$H_v = MD5\left[SE_{Data}\right]$$

4. The security personnel's request is then encrypted with the target government department's public key in order to avoid others from hacking or altering the request. As the request is encrypted with the target department's public key, it can be decrypted and viewed only by the target department.

$$S_{Query} = Enc\left[\text{Query}\right]_{k_R^{Pub}}$$

5. The hash value H_v, the set of random values R and the encrypted request S_{Query} are combined and encrypted with the security personnel's private key $K_S^{\Pr i}$ to obtain SA_{Data}. The encryption with the security personnel's private key genuinely authenticates the security personnel's request.

$$SA_{Data} = Enc\left[\text{R} + \text{S}_{\text{Query}} + H_v\right]_{k_S^{\Pr i}}$$

6. The encrypted random number E_{RV} and the obtained SA_{Data} are combined and encrypted with the public key K_C^{Pub} of the master control to form the security personnel's request S_{msg}

$$S_{msg} = Enc[E_{RV} + SA_{Data}]_{k_C^{Pub}}$$

The structured security personnels' request S_{msg} contains the encrypted random number E_{RV}, and the obtained SA_{Data}, all encrypted with the master control's public key K_C^{Pub}. Now, this structured request S_{msg} is transmitted to the master control. The block diagram in Figure 1 shows the steps involved in structuring the security personnel's request.

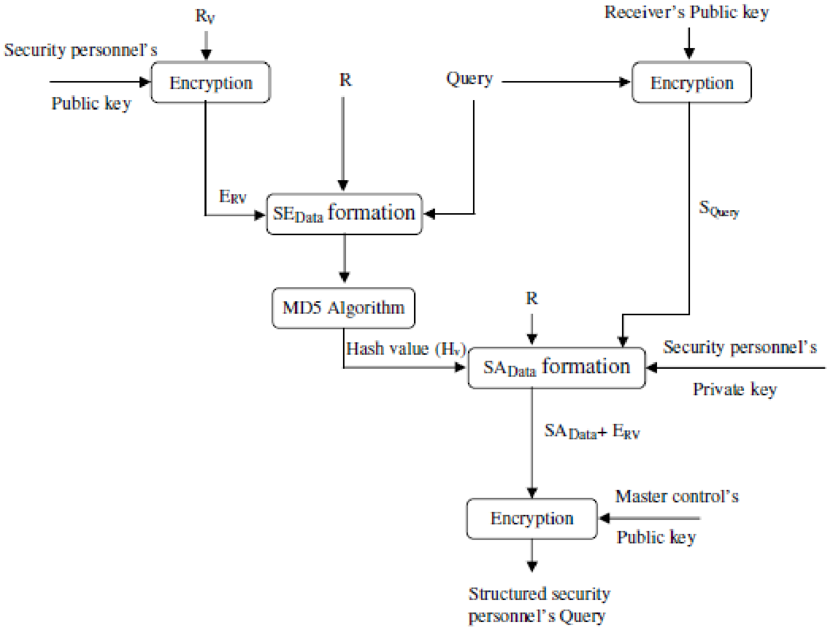

Figure 1: Structuring of the security personnel's request

B. Steps in the proposed approach at the Master Control

1) Validation of the security personnel's request

On receiving the request from the security personnel, the master control must authenticate the security personnel followed by validating the integrity of the security personnel's request. Then, the master control will add its identity to the request and send the same to the target government department. The block diagram in Figure 2 shows the steps involved in the validation of the security personnel's request by the master control.

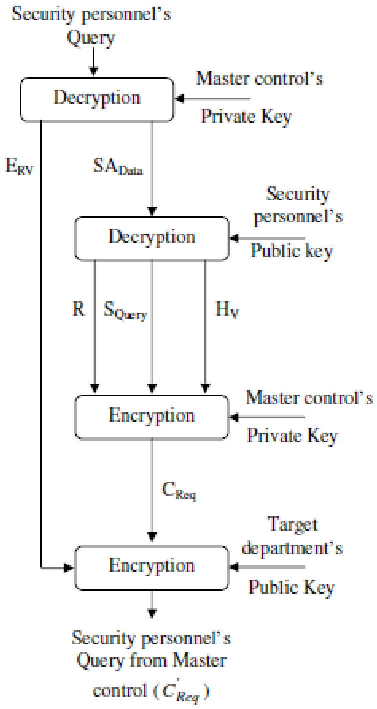

Figure 2: Validation of the security personnel's request by the Master control

The steps involved in the integrity checking and authentication of the security personnel's request are as follows:

1. The request from the security personnel S_{msg} is first decrypted using the master control's private key K_C^{pri}. Since the security personnel's original request is encrypted with the public key of the target government department, it couldn't be viewed by the master control. As the private key is the secret property of the intended target, the target is assured that no one else can decrypt the request.

$$SC_{msg} = Dec\lfloor S_{Msg} \rfloor_{k_C^{\Pr i}}$$

2. The SC_{msg} obtained from the above step contains SA_{Data} and E_{RV}. The SA_{Data} is then decrypted with the public key K_S^{Pub} of the security personnel. The successful decryption authenticates that the request has originated from the claimed security personnel.

$$SC'_{msg} = Dec[SA_{Data}]_{k_S^{Pub}}$$

$$SA_{Data} = \lfloor E_{RV} + R + S_{Query} + H_V \rfloor$$

The SC'_{msg} contains the set of random values R, the encrypted random number E_{RV}, the encrypted request S_{Query} and the hash value H_V.

3. Then, the set of random values R, the encrypted request S_{Query} and the hash value H_V are combined and encrypted using the master control's private key $K_C^{\Pr i}$ to obtain C_{Req}.

$$C_{\text{Req}} = Enc\lfloor R + S_{Query} + H_V \rfloor_{k_C^{\Pr i}}$$

4. Subsequently, the master control forms C'_{Req} by combining the encrypted random number E_{RV} and the formed C_{Req} and then encrypting them with the public key of the target department K_R^{Pub}. Finally, the formed C'_{Req} will be sent to the target department.

$$C'_{\text{Req}} = Enc[E_{RV} + C_{\text{Req}}]_{k_R^{Pub}}$$

C. Steps in the proposed approach at the Target Department

1) Validation of the request by the Target Department

After receiving the security personnel's request from the master control, the target department must authenticate the master control and the security personnel followed by validating the integrity of the security personnel's request. The steps involved in the above processes are as follows:

1. The request C'_{Req} received from the master control is first decrypted with the private key of the target department to obtain R_{msg}. The R_{msg} consists of the encrypted random number E_{RV} and the C_{Req}.

$$R_{msg} = Dec\lfloor C'_{\text{Re}\,q} \rfloor_{K_R^{pri}}$$

$$R_{msg} = E_{RV} + C_{\text{Re}\,q}$$

2. Next, the C_{Req} is decrypted with the public key of the master control to obtain R'_{msg}. The R'_{msg} contains the set of random values R, the encrypted request S_{Query} and the hash value H_V.

$$R'_{msg} = Dec[C_{\text{Re}\,q}]_{K_C^{Pub}}$$

$$R'_{msg} = R + S_{Query} + H_V$$

3. Then, the actual query from the security personnel S_{Query} is decrypted with the target department's private key, since S_{Query} is encrypted with the public key of the target department.

$$R''_{msg} = Dec[S_{Query}]_{K_R^{\Pr i}}$$

4. Subsequently, the set of random values R, the actual query R''_{msg} and the encrypted random number E_{RV} are combined and their hash value $\overline{H_V}$ is computed with the aid of the MD5 algorithm.

$$\overline{H_V} = MD5[E_{RV} + R + R'_{msg}]$$

5. If the hash value $\overline{H_V}$ computed from the above step and the hash value H_V present in the security personnel's request are identical, it guarantees that the request has not been tampered during the transfer.

```
If $H_V == \overline{H_V}$ then
    Query is not tampered
else
    Query is tampered
end if
```

The block diagram in Figure 3 depicts the steps involved in the validation of the security personnel's request by the target department.

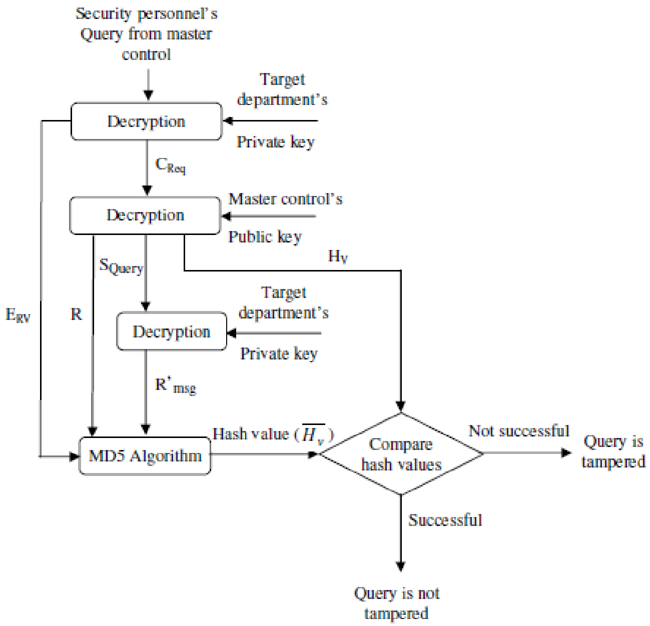

Figure 3: Validation of the security personnel's request by the target department

2) Structuring of response to the Security Personnel's query

After successful validation of the security personnel's request, the target department will form response for the security personnel's query. The steps involved in structuring the response are as follows:

1. The target department's database is scanned once to attain the rank of the security personnel, from whom the request originated. The rank symbolizes the level of security personnel, and it decides the credibility of the information that must be given to the security personnel.

2. The encrypted random number E_{RV} in the security personnel's request will be kept as such in the response.

3. A mapping function M_{fn}, uniquely defined between the communicating parties is retrieved from the target department's database. For each security personnel, there is a unique mapping function in the target department's database. Then, the obtained mapping function is applied on the set of random values R in the security personnel's request to attain mapping value M_{val} . Subsequently, its sine value is computed and represented as M'_{val}.

$$M_{val} = M_{fn}(R)$$

$$M'_{val} = Sin(M_{val})$$

where $R = \{r_1, r_2, r_3, ..., r_n\}$, $M_{fn} = \{+,-,*,/\}$

4. Subsequently, the target department determines the amount and credibility of confidential information to be shared with the security personnel on the basis of the security personnel's rank obtained from Step 1.

5. The response corresponds to the security personnel's request; the calculated mapping value and the encrypted random number E_{RV} are combined to form RE_{Data}.

$$RE_{Data} = [E_{RV} + M'_{val} + Answer]$$

6. With the aid of the MD5 Algorithm, the hash value H_v is calculated from the RE_{Data}

$$H_v = MD5[RE_{Data}]$$

7. The response corresponds to the security personnel's request is then encrypted with the public key of the security personnel K_S^{Pub}, so that it can only be viewed by the security personnel.

$$S_{Answer} = Enc[\text{Answer}]_{k_S^{Pub}}$$

8. The encrypted response S_{Answer}, the encrypted random number E_{RV}, the mapping value M'_{val} and the hash value H_v are combined and encrypted with the master control's public key K_C^{Pub} to form R_{Res}. Finally, the formed R_{Res} will be sent to the master control.

$$R_{Res} = Enc[E_{RV} + M'_{val} + S_{Answer} + H_v]_{k_C^{Pub}}$$

The block diagram in Figure 4 illustrates the steps involved in structuring the response to the security personnel's request.

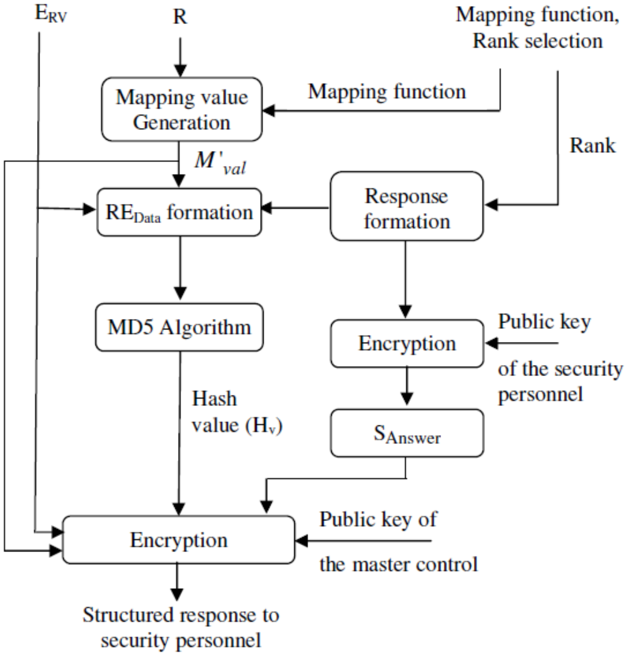

Figure 4: Structuring of response to the security personnel's query

D. Steps in the proposed approach at the Master Control

1) Validation of Target Department's Response by the Master Control

On receiving response from the target department, the master control must make sure the following: 1) integrity of the target department's response 2) The response originated from the true or intended target (Authentication). The steps involved in the above processes are as follows:

1. The target department's response R_{Res} is first decrypted with the master control's private key K_C^{Pri}, which discloses the encrypted random number E_{RV} , mapping value M'_{val}, the encrypted response S_{Answer} and the hash value H_v .

$$RC_{msg} = Dec[R_{\mathrm{Res}}]_{k_C^{\mathrm{Pri}}}$$

$$RC_{msg} = E_{RV} + M'_{val} + S_{Answer} + H_v$$

2. The mapping value is recomputed at the master control side and compared with the mapping value present in the response to ensure that the response came from the intended target department.

```
If  $\mathrm{M'}_{\mathrm{val}} = \overline{\mathrm{M'}_{\mathrm{val}}}$  then
        The target is valid and forward the response
else
        Discard the response
end if
```

3. After the validation of the intended target, the encrypted response, the encrypted random number, mapping value and the hash value are combined and encrypted with the public key of the security personnel K_S^{Pub} and is sent back to the security personnel.

$$CS_{msg} = Enc[E_{RV} + M'_{val} + S_{Answer} + H_v]_{k_S^{Pub}}$$

The block diagram in Figure 5 shows the steps involved in the validation of target department's response by the master control.

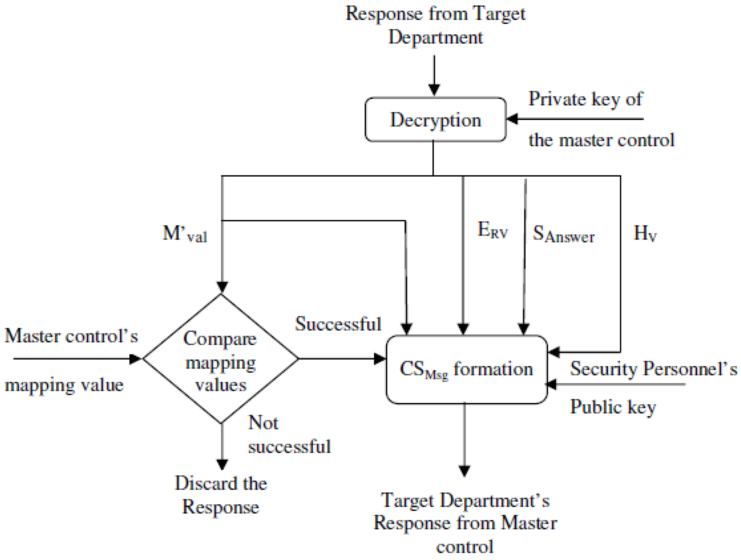
Response from Target Department
Decryption
Private key of the master control
M'val
ERV
SAnswer
HV
Master control's mapping value
Compare mapping values
Successful
CSMsg formation
Security Personnel's Public key
Not successful
Discard the Response
Target Department's Response from Master control

Figure 5: Validation of Target Department's response by the Master control

E. Steps in the proposed approach at the security personnel side

1) Validation of Target Department's Response by the Security Personnel

On the reception of the response from the master control, the security personnel must ensure the following: 1) integrity of the target department's response 2) The response originated from the true or intended target (Authentication). 3) The response corresponds to the apt request of the security personnel. The steps involved in the above processes are as follows:

1. The received response CS_{msg} is first decrypted with the security personnel's private key K_S^{Pri}.

$$S_{\mathrm{Res}} = Dec[CS_{msg}]_{k_S^{\mathrm{Pri}}}$$

2. The response is confirmed for its integrity by computing the hash value and comparing it with the hash value from the target department.

$$\overline{H_v} = MD5[E_{RV} + M'_{val} + Answer]$$

```
If  $H_v == \overline{H_v}$  then
        information is not tampered
```

```
else
        information is tampered
end if
```

3. The encrypted random number in the target department's response is decrypted with the private key of the security personnel $K_S^{\text{Pr}\,i}$ to make sure that the response is valid for the request made.

```
if (RV == $\text{Dec}[\text{E}_{\text{RV}}]_{K_S^{\text{Pr}\,i}}$)
        The response is valid
end if
```

4. After evaluating all the parameters in the target department's response, the security personnel considers it as a valid response from the valid target department.

The block diagram in Figure 6 shows the steps involved in the validation of target department's response by the security personnel.

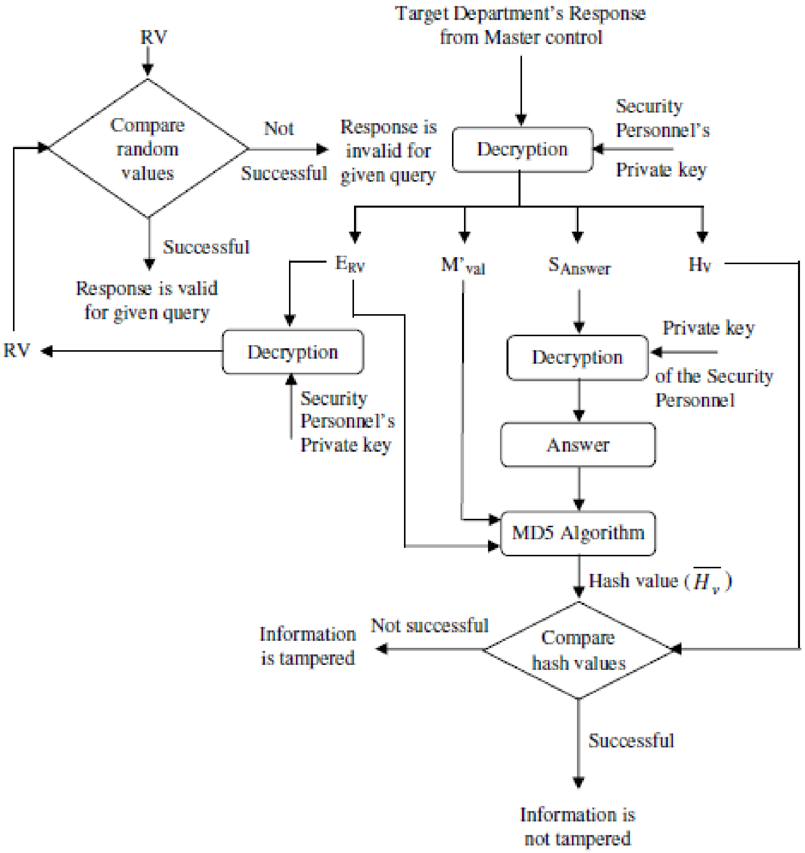
RV
Compare random values
Not Successful
Response is invalid for given query
Successful
Response is valid for given query
RV
Target Department's Response from Master control
Decryption
Security Personnel's Private key
E_RV
M'_val
S_Answer
Hv
Decryption
Security Personnel's Private key
Decryption
Private key of the Security Personnel
Answer
MD5 Algorithm
Hash value ($\overline{H_v}$)
Compare hash values
Not successful
Information is tampered
Successful
Information is not tampered

Figure 6: Validation of Target Department's response by the Security personnel

All the above steps guarantee that the proposed role and cooperation based approach is effective in providing confidential, authenticated and secure information sharing. Further communications between the security personnel and the government intelligence departments follow the approach discussed above.

IV. Experimental Results

The results obtained from the experimentation on the proposed secure information sharing approach are presented in this section. The presented role and cooperation based information sharing approach is programmed in Java (JDK 1.6). The results acquired from the experiments show that the presented approach provides effective and secure information sharing for security personnels and the government intelligence departments. The master control introduced in the proposed approach enhances the security of information sharing by monitoring and controlling the information exchanged between the security personnel and the government intelligence departments. The process started with a request for confidential information about a person, by utilizing the techniques of hashing, a unique mapping function and public key cryptography. The master control monitored and controlled both the request and response from the security personnel and the government intelligence department. The target department after a security verification responded with the suitable information on the basis of the rank of the security personnel. The information shared will be a subset of the information available with the target department based on the rank of the security personnel.

TABLE 1: RESULTS OF EXPERIMENTATION

Security Personnel	Government Intelligence Department	Unique Identifier	Available Information	Rank-based shared information
P1	IB	1	{23,37,39,43,38,37,24,38,35,29,40,31,33,76,48,21,52,67,52,71,49,26,15,38,24}	{23,37,39,43,38}
P1	CBI	2	{39,33,46,56,74,46,49,50,59,14,6,18,29,43,67,45,69,58,60}	{39,33,46,56,74}
P1	NCB	3	{39,35,42,57,65,49,52,64,77,87,90,78,64,59,73,75,68,13,17,19,24,29}	{39,35,42,57,65}
P2	CBI	1	{19,17,36,14,23,35,47,34,63,31,22,40,19,12,26,18,13,17,27,46,23,25,18,29,30}	{35,47,34,63,31,22,40}
P2	CID	3	{62,68.65,54,57,34,31,30,28,26,7,16,13,27,29,44,47,54,52,39}	{34,31,30,28,26}
P3	CID	3	{62,68.65,54,57,34,31,30,28,26,7,16,13,27,29,44,47,54,52,39}	{7,16,13,27,29}
P3	IB	2	{15,9,17,28,30,85,31,17,49,27,32,46,26,23,25,28,22,29,30,12,7,19,13,28,31}	{26,23,25,28,22,29,30}
P3	NCB	1	{11,26,33,15,17,45,13,17,18,28.24.32,7,48,26,45,76,82,37,21,28,17,19,25}	{7,48,26,45,76,82}
P4	CBI	2	{39,33,46,56,74,46,49,50,59,14,6,18,29,43,67,45,69,58,60}	{67,45,69,58,60}
P4	IB	1	{23,37,39,43,38,37,24,38,35,29,40,31,33,76,48,21,52,67,52,71,49,26,15,38,24}	{52,71,49,26,15,38,24}

Table 1 depicts the results obtained from the experimentation on the proposed secure information sharing approach using duplicate data. From the table, it is obvious that the quantity of information shared between the communicating parties depends on the rank of the security personnel. In Table 1, the field *Available Information* contains the confidential information about the persons and their suspicious activities, which has been collected over long periods of time and the field *rank-based shared Information* consists of the information shared between the security personnel and the government intelligence departments. The proposed approach successfully preserved the privacy of the person whose information is exchanged between the communicating parties.

V. CONCLUSION

Information sharing and integration are being looked upon as the most increasingly adopted methodologies by governments around the world, for solving problems in a broad variety of programs and policy areas. Secured information exchange is a significant characteristic of any digital government that wants to assure democratic principles. Challenges in building a computational infrastructure for exchanging top secret information is difficult to solve and demand novel incentive schemes. In this paper, we have presented an efficient role and cooperation based approach for confidential sharing of secret information amongst security personnels and government departments. The proposed secure information sharing approach has offered confidentiality, authentication, integrity and agency verification by utilizing MD5 Algorithm, public key infrastructure and a unique and complex mapping function. Also, on the basis of a predefined rank of security personnel, a restricted privacy is maintained between the security personnel and government intelligence departments. The effectiveness of the proposed approach has been demonstrated with the help of experimental results.

REFERENCES

[1] Digital Government, “Directorate for Computer and Information Science and Engineering Division of Experimental and Integrative Activities”, NSF-02-156, November 7, 2002.

[2] Z. Fang, “E-Government in Digital Era: Concept, Practice, and Development”, International Journal of the Computer, The Internet and Management, Vol. 10, No.2, pp: 1-22, 2002.

[3] Robert D. Atkinson, "Digital Government: The Next Step to Reengineering the Federal Government", DC: Progressive Policy Institute, 2000.

[4] Jane E. Fountain, "Preventing Chronic Disease, public health research, Practice, and Policy", Vol. 1: No. 4, October 2004.

[5] F.Arcieri, G.Melideo, E.Nardelli and M.Talamo, "Experiences and issues in the realization of e-government services", Proceedings of the 12th Int'l Wrkshp on Research Issues in Data Engineering: Engineering e-Commerce/ e-Business Systems, pp: 1066-1395, 2002.

[6] James B. D. Joshi, Arif Ghafoor, Walid G. Aref and Eugene H. Spafford, "Security and Privacy Challenges of a Digital Government", Advances in Digital Government–Technology, 2002.

[7] Guido Bertucci, "Managing Knowledge To Build Trust In Government", United Nations Department of Economic and Social Affairs, United Nations Publication, New York, 2007.

[8] Policy Guideline on Information Sharing, Royal Government of Bhutan Ministry of Information & Communications, September 2006.

[9] Athman Bouguettaya, Mourad Ouzzani, Brahim Medjahed, Ahmed Elmagarmid, "Supporting Data and Services Access in Digital Government Environments", 2002.

[10] Fillia Makedon, Calliope Sudborough, Beth Baiter, Grammati Pantziou and Marialena Conalis-Kontos, "A Safe Information Sharing Framework for E-Government Communication”, IT white paper from Boston University, 2003.

[11] NASCIO, Call for Action, “A Blueprint for Better Government: The Information Sharing Imperative", May 2005.

[12] Thomas Casey, Alan Harbitter, Margaret Leary, and Ian Martin, “Secure information sharing for the U.S. Government”, White papers,. Nortel Technical Journal, 2008.

[13] Peng Liu and Amit Cheta.l, “Trust-Based Secure Information Sharing Between Federal Government Agencies”, Journal of the American Society for Information Science and Technology, Vol 56, Issue 3, pp: 283 – 298, 2005.

[14] Fillia Makedon, Calliope Sudborough, Beth Baiter, Grammati Pantziou and Marialena Conalis-Kontos, "A Safe Information Sharing Framework for E-Government Communication", IT white paper from Boston university, 2003.

[15] Jing Fan, Pengzhu Zhang, "A Conceptual Model for G2G Information Sharing in E-Government Environment", 6th Wuhan International Conference on E-Business, Wuhan (CN), 2007.

[16] Xin L., "Distributed Secure Information Sharing Model for E-Government in China," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), Vol. 3, pp: 958-962, 2007.

[17] Nabil R. Adam, Vijay Atluri, Soon Ae Chun, John Ellenberger, Basit Shafiq, Jaideep Vaidya, Hui Xiong, "Secure information sharing and analysis for effective emergency management", Proceedings of the international conference on Digital government research, Vol. 289, pp:407-408 ,2008.

[18] Nabil Adam, Ahmet Kozanoglu, Aabhas Paliwal, Basit Shafiq, "Secure Information Sharing in a Virtual Multi-Agency Team Environment", Electronic Notes in Theoretical Computer Science, Vol: 179, pp: 97-109, 2007.

[19] 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.

[20] Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang, "Secure information sharing enabled by Trusted Computing and PEI models", Proceedings of the ACM Symposium on Information, computer and communications security, pp: 2 - 12, 2006.

[21] Tryg Ager, Christopher Johnson, Jerry Kiernan, "Policy-Based Management and Sharing of Sensitive Information among Government Agencies," MILCOM 2006, pp: 1-9, 2006.

[22] Thomas Casey, Alan Harbitter, Margaret Leary, and Ian Martin, "Secure information sharing for the U.S. Government", white paper, Nortel Technical Journal, 2008.

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

[24] Peng Liu and Amit Chetal, “Trust-Based Secure Information Sharing Between Federal Government Agencies”, Journal of the American Society for Information Science and Technology, Vol.56, No. 3, pp. 283 – 298, 2005.

[25] Rakesh Agrawal, Alexandre Evfimievski, Ramakrishnan Srikant, "Information Sharing Across Private Databases", In SIGMOD '03: Proceedings of the 2003 ACM SIGMOD international conference on Management of data, pp. 86-97, 2003.

[26] Ryan Layfield, Murat Kantarcioglu, Bhavani Thuraisingham, "Incentive and Trust Issues in Assured Information Sharing", International Conference on Collaborative Computing, 2008.

[27] Guido Bertucci, "Managing Knowledge To Build Trust In Government", United Nations Department of Economic and Social Affairs, United Nations Publication, New York, 2007.

[28] Theresa A. Pardo, “Collaboration and Information Sharing: Two Critical Capabilities for Government”, Center for Technology in Government, University at Albany Annual Report, 2006.

[29] Md.Headayetullah, G.K. Pradhan, "A Novel Trust-Based Information Sharing Protocol for Secure Communication between Government Agencies", European Journal of Scientific Research, Vol: 34, No: 3, pp: 442-454, 2009.

[30] Md.Headayetullah, G.K. Pradhan, "Secure Information Sharing Between Government Intelligence Agencies: An Innovative Protocol Based on Trust", International Journal of Engineering and Technology, Vol: 1, No: 4, pp: 346, 2009.

[31] Gail-Joon Ahn, Badrinath Mohan, Seng-Phil Hong, "Towards secure information sharing using role-based delegation", Journal of Network and Computer Applications, Vol: 30, No:1, pp: 42 - 59, January 2007.

[32] Mudhakar Srivatsa, Dakshi Agrawal, Steffen Reidt, "A metadata calculus for secure information sharing", Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, pp: 488-499 , 2009.

[33] 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.

Md.Headayetullah received the Diploma in Computer Science & Engineering (DCSE) with 1st Class from Acharya Polytechnic, Bangalore, India and Bachelor of Engineering (B.E) degree with 1st Class from Yeshwantrao Chavan College of Engineering of Nagpur University, Nagpur, India in 2000 and 2003 respectively. He received second prize in state level for his best project in B.E degree. He received M.Tech degree with First Class with Honours from the Department of Computer Science & Engineering and Information Technology of Allahabad Agricultural Institute-Deemed University, Allahabad, India in 2005. He was the topper of the University in his M.Tech Degree. He is currently pursuing the PhD (Computer Sc. & Engineering) degree, working closely with Prof. (Dr.) G.K Pradhan and Prof. (Dr.) Sanjay Biswas in the Department of Computer Science and Engineering from Institute of Technical Education & Research (Faculty of Engineering) of Siksha O'Anusandhan University (SOAU), Bhubaneswar, India. He works in the field of E-Government, Digital Government, Networking, Internet Technology, Data Privacy, Cryptography, Information Security and Mobile Communication. He has authored more than four Research Publication in International Journal. He is currently working as an Assistant Professor in Computer Science & Engineering and Information Technology at Dr. B.C. Roy College of Engineering, Durgapur, West Bengal University of Technology, Kolkata, India. Professor, Headayetullah is the members of IAENG and IACSIT respectively.

G.K. Pradhan received the PhD degree from Indian Institute of Technology (IIT) Kanpur, India. He served as a lecturer, Assistant Professor and Associate Professor in several Institutes in India. Dr. Pradhan is currently working as a Professor in Computer Science & Engineering and Information Technology at Institute of Technical Education & Research (Faculty of Engineering) of Siksha O Anusandhan University (SOAU), Bhubaneswar, India. He is working as a Chair person of Doctoral Scrutiny Committee (DSC) of Institute of Technical Education & Research (Faculty of Engineering) of Siksha O Anusandhan University, Bhubaneswar, India. Dr. Pradhan serves as a research supervisor for PhD degree in the field of Computer Science and Engineering and mathematics. He has authored several books and had more than 25 research publication in Journal. His fields of interests are Software Engineering, E-Commerce, E-Business Application, Digital Government, Internet Technology and Mobile Communication.