International Journal of Engineering and TechnologyVol. 1, No.4 ,October, 2009
ISSN: 1793-8236

Secure Information Sharing Between Government Intelligence Agencies: An Innovative Protocol Based on Trust

Md.Headayetullah and G.K. Pradhan

Abstract—**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. Issues of universal concern such as disease detection and control, terrorism, immigration and border control, illicit drug trafficking, and more demand information sharing, coordination and collaboration amid government agencies within a country and across national boundaries. Several daunting challenges exist towards the development of a competent information sharing protocol. The principal challenge would be the development of a protocol capable of sharing secure information between different government and non-government agencies, with the purpose of streamlining government services. In this paper, we devise an innovative and proficient trust-based information sharing protocol for secure exchange of confidential and top secret information amongst government intelligence agencies across national boundaries using public key cryptography. The proposed protocol makes use of 1) MD5 Algorithm for Data Integrity 2) Public key cryptosystem for Confidentiality and Authentication and 3) A unique and complex mapping function for Agency Identification. Furthermore, the proposed protocol facilitates privacy preserving information sharing with probable restrictions based on the trust level maintained between the communicating agencies. The trust protocol devised ensures secure and stream-lined information sharing among government intelligence agencies to shun ominous activities.**

—Digital Government, Government Intelligence Agencies, Information Sharing, Mapping Function, Message Digest 5 (MD5), Public-Key Cryptosystem, Terrorism, Security, Trust.

I. INTRODUCTION

Government is a chief accumulator and contributor of data and information, provider of information–based services and consumer of information technologies [1]. The ever so important next step in reinventing government is the universal application of information and communications technologies for the delivery of government services, in short, nurturing digital government [8]. Digital Government is defined as the "civil and political conduct of government, including provision of services, by utilizing information and communication technologies" [2].

The initiatives of digital government are complex change efforts anticipated to utilize innovative and emerging technologies to support transformations in the operation and effectiveness of government [10]. Digital government, intended to optimize its internal and external functions with the aid of Information Technology (IT), proffers a set of tools to the government, the citizen and business that can effectively renovate the means of interaction, service delivery, knowledge utilization, policy development and implementation, participation of citizens in governance, and reforms in public administration and good governance goals are achieved [9]. Information is one of the most noteworthy assets of government. As a result, governments around the world opt for information sharing as a strategy for increasing the value of information in offering services and reacting to problems [21], [26].

Potential for booming government information technology (IT) innovations is particularly important when collaboration and information sharing across domains are vital to success [3]. "Information sharing" to different government sectors means different things at different periods of time. The information can be defined as: collection and sharing of intelligence between two security divisions, or sharing actual e-crime data, data observations, notes of surveillance, scientific facts, commercial transaction data, and more. Given that there is a shortage of standard methods for digital government information sharing, the means of information sharing are not presently monitored, authenticated and recorded on a regular basis [23], [27]. Several daunting research challenges persist in information systems that offer international collaborations amongst governments: information management across agencies and organizations, transparent interoperation across heterogeneous information networks, and share of multilingual information [11], [12], [28]. Besides, information sharing is not at all times assured to be free from risks, which may comprise unauthorized access, malicious alteration, and destruction of information or misinformation, computer intrusions, copyright infringement, privacy violations, human rights violations and more.

One of the most essential issues for the creation of effectual e-government architecture is confidential sharing of information among diverse government agencies. In modern times, the government agencies countenance a number of complex global problems like: border control, illegal immigration, terrorism, and bio-security threats. The complex global problems aforesaid could be prospectively solved by effectual collaboration and information sharing amongst the agencies [4]. Information sharing is imperative to enhance the security of the country and is a significant factor in proposing absolute and practical approaches for protection against imminent terrorist attacks. Terrorism is definitely one of the striking problems all over the world [18], and it is found that an effectual and secure information sharing system among global intelligence agencies will make possible a much more stern control over Terrorism. There have been so many occurrences of terrorist attacks witnessed

all over the world that would have been prevented by efficient trust-based information sharing.

Terrorism has reached staid dimensions after the twin towers attack on September 11 at the World Trade Centre in United States of America (USA). The whole world came across the complete blown up pictures that portrayed the sudden vertical collapse of the commercial might of USA. The September 11 attack and the following investigations revealed the existence of a grave information sharing problem among the pertinent federal government agencies, and the problem could cause large dearth in terrorism attack detection [14]. On 26 November, 2008, the world witnessed another most publicized sudden crisis, which was an outburst of anti social activity against common people of India, where more than a couple of hundred were dead and several hundreds were injured [20]. The above are some serious catastrophes that forced the global intelligence agency authorities to repeatedly emphasize the necessity for a more efficient information sharing system. A secure and trusted information-sharing infrastructure is a prerequisite to facilitate government agencies to interact with and share information effortlessly and impeccably across many different networks and databases nationwide [5], [13]. Creating a broad foundation for information sharing necessitates trust amongst all information sharing partners. The apprehension that shared information will not be safeguarded effectively or used duly; and that sharing will not always occur mutually, are grounds for lack of trust [14].

History reveals evidences of information sharing that have occurred in a very restricted manner amongst law enforcement agencies: on the whole, only by individual to individual or case by case basis. Efficient sharing of information between different communities at varied levels of government – national, state, regional, and local – has developed into a pinnacle priority of world governments, whose leaders continually emphasize the necessity for more effective information sharing to enhance homeland security efforts [14]. There are two categorizes of information sharing technologies currently, they are: (a) privacy-preserving information sharing, where two communicating parties with information x and y respectively communicate with each other such that a function of x and y, symbolized f(x,y) is computed and shared by the two parties, preserving the privacy of x and y and (b) non-privacy-preserving information sharing, where two communicating parties with information x and y respectively share (part of) x and/or (part of) y along with f(x,y) [29, 30].

The potential to share terrorism-related information can achieve a unification of the federal, state, and local government agencies efforts, as well as the private sector in forestalling or reducing terrorist attacks. Many government agencies abandon to share information primarily because of 1) internal conflicts 2) fear of impairing their individual national interests and 3) most substantially the fear of information being hacked. Information exchange between government agencies necessitates a distinct, more restraining trust model primarily because of two reasons: (1) Presence of extremely sensitive information (2) the demand for a more accountable and fair information sharing mechanism to surmount the differences and conflicts-of-interest existing between agencies [14]. All these factors insist the need for a trust-based effective information sharing system. Albeit trust-based information access is well studied in the literature [19, 15, 16, 17, 7] the presented trust models, which are based on certified attributes, could not proffer effectual information sharing among government agencies.

This work is an enhanced version of our previous research [35], which improves the security of the presented trust-based security protocol by providing authentication, for confidential exchange of top secret information among global government intelligence agencies without harming their own national interests. As a universal rule, digital government principles are based on the surmise that distinct government agencies are ready to collaborate and share their findings through a common network infrastructure. A secluded means to help information transfer fosters the courage and co-operation amongst the government intelligence agencies. The government intelligence agencies can efficiently share information about terrorists and their activities in a confidential manner by means of the proposed trust-based security protocol. The precision and the amount of information shared between communicating government intelligence agencies is based on the predefined trust level maintained. The proposed security protocol achieves data integrity using MD5 Algorithm, confidentiality and authentication using public key infrastructure, controlled privacy using trust level and agency verification using a mapping function.

The rest of the paper is organized as follows: A brief review of the researches related to the development of trust-based protocols for secure information sharing among communicating parties is presented in Section 2. The proposed trust-based protocol for effectual and confidential information sharing is presented in Section 3. Section 4 discusses the experimental results obtained and finally the conclusions are summed up in Section 5.

II. REVIEW OF PRIOR RESEARCHES

A copious number of trust-based information sharing protocols has been offered by researchers for effective information sharing between communicating parties. Of them, a handful of researches deal with secure sharing of confidential information among government agencies. The development of trust-based secure information sharing protocols is one of the leading research areas. Here, we present a concise review of selected significant contributions from the existing literature.

Peng Liu et al. [14] have proposed a novel interest-based trust model and an information sharing protocol to surmount the problem of information sharing between government agencies. The proposed protocol incorporated a family of information sharing policies, along with information exchange and trust negotiation, interleaved and interdependent upon each other. Furthermore, the protocol was implemented by making use of the emerging technology of XML Web Services. The implementation was completely compatible with the Federal Enterprise Architecture reference models and can be integrated openly into presented E-Government systems.

Jing Fan et al. [25] have presented a conceptual model for information exchange in an e-government infrastructure. They deduced that the Government-Government (G2G) information sharing model will help in offering an understanding for G2G information sharing and will assist decision makers in framing decisions with regards to participation in G2G information sharing. They tested the proposed conceptual model with the intention of discovering the factors persuading the participation in an e-government information sharing and emphasizing the conceptual model via case study under Chinese government system.

Fillia Makedon et al. [23] have presented a negotiation-based sharing system called SCENS: Secure Content Exchange Negotiation System developed at Dartmouth College with the assistance of many interdisciplinary experts. SCENS was a multilayer scaleable system that brings about surety to transaction safety via numerous security mechanisms. It was based on a metadata description of heterogeneous information and was applied to a number of diverse domains. They demonstrated that with susceptible and distributed information the government users might bring about an agreement on the conditions of sharing information by means of negotiation.

Xin L. [22] has devised a distributed information sharing model and also assessed the technique standard support of the model. It was deduced that the cost of managing the government information exchange and cooperation between agencies will be decremented with an augment in the ability and efficiency of agencies' collaboration owing to the secure e-government information sharing solutions. Nabil R. Adam et al.[32] have studied on confronts in integration, aggregation and secure sharing of information for offering situation awareness and response at the strategic level. The proposed system based on context-sensitive parameters, filters, integrates, and proficiently visualizes the data extracted from different autonomous systems essential to get a common operational picture. One noteworthy confront found was to make certain secure information sharing. Information sharing remains to be a principal intricacy owing to the data privacy and ownership concerns and an extensive range of security policies adopted within different government agencies.

Nabil Adam et al.[33] have presented a two tier RBAC approach to offer security and discriminative information sharing between virtual multi-agency response team (VMART) and as requirements arise it allows VMART expansion by admittance of new collaborators (government agencies or NGOs). They also provided a coordinator Web Service for each member agency. The coordinator Web Service works with the following responsibilities: 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 XML document encryption in compliance with equivalent XML schema defined RBAC policies.

Achille Fokoue et al. [34] have devised logic for risk optimized information sharing by utilizing rich security metadata and semantic knowledge-base that encapsulates domain specific concepts and relationships. They demonstrated that the approach was: (i) flexible: e.g., tactical information decay sensitivity in correspondence with space, time and external events, (ii) situation-aware: e.g., encodes need-to-know based access control policies, and more importantly (iii) assists explanations for non-shareability; these explanations with rich security metadata and domain ontology allows a sender to astutely achieve information transformation with the intention of sharing the transformed information with the recipient. Furthermore, they have provided a secure information sharing architecture making use of a publicly available hybrid semantic reasoner and also presented a number of descriptive examples that accentuates the advantages of the approach in comparison to traditional approaches.

Ravi Sandhu et al. [24] have proposed the ways by which modern Trusted Computing (TC) technologies could facilitate secure information sharing, those not offered with pre-TC technology. They have created the PEI framework of policy, enforcement and implementation models, and demonstrated its application in examining the problem and synthesizing solutions for it. The framework facilitated the detailed examination of potential TC applications for secure information sharing in their future work.

Tryg Ager et al. [31] designed a set of policy-based technologies to ease increased information sharing between government agencies without negotiating information security or individual privacy. The approach includes: (1) fine-grained access controls that support deny and filter semantics for complex policy condition satisfaction; (2) a sticky policy ability that facilitates consolidation of information from multiple sources subject to the source's original disclosure policies of each; (3) a curation organization that permit agencies to apply and contrive item-level security classifications and disclosure policies; (4) an auditing system that accounts for the curation history of each information item; and (5) a provenance auditing method that traces information derivations over time to offer support in evaluating information quality. The eventual aspiration was to offer a scope to solve stupendous information sharing problems in government agencies and proffer direction for the development of future government information systems.

III. SECURE INFORMATION SHARING PROTOCOL BASED ON TRUST

Government information is a vital asset that must be maintained in trust and efficiently managed by governments. A superior importance has to be put forth by government institutions, at all levels, on the sharing of data and information between and amongst its trusted partners. With the purpose of meeting the rising demands and service expectations, information must be influenced and supported by coordinated, integrated solutions [6]. With dexterous information sharing solutions, government intelligence agencies will be competent to predict the security risks and attacks, including terrorist attacks. Nevertheless, devising secure information sharing mechanism between government intelligence agencies is not trivial because they worry that their interests may be exposed when their information is shared with other agencies [22]. This section presents the

proposed innovative and proficient trust-based security protocol for secure sharing of confidential information among government intelligence agencies.

The devised protocol is non privacy-preserving, but assures that both the source and the target agencies are ensured paramount confidentiality and authentication in information transfer. The intelligence agencies fret that the hacking of sensitive information shared would cause apprehension to their own national interests. This demands an efficient security protocol that offers confidential and authenticated information sharing with regards to the national interests of both the source and the target government agencies. Furthermore, there is likelihood that the target agency would misuse the secret information without the apt approval of the source agency. The above case cannot be entirely averted in a non privacy-preserving protocol but could be controlled by availing information transfer based on the predefined trust level existing between the communicating government agencies. The government intelligence agencies make use of the devised protocol to share terrorist information in a secure manner. The credibility of information shared is based on the trust level maintained between communicating government intelligence agencies. The proposed protocol ensures trust-based secure information exchange between communicating agencies.

The prerequisites for the proposed trust-based security protocol includes: a) The public keys of the communicating agencies b) A unique and complex mapping function. The communicating agencies attain their public and private keys from a trusted Certificate Authority (CA). The predefined complex mapping function uniquely identifies the communicating agencies. The steps describing the proposed trust-based security protocol is organized in such a way that, the source agency first requests for some secret and valuable information followed by the corresponding target response based on the trust level maintained and a validation of the target response at the source agency.

A. Steps in the Protocol at Source Agency

1) Structuring of Source Request

The source agency requests for some surreptitious information about terrorists and their suspicious activities to the target agency. It is the duty of the source agency 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 framing of the source request involves the following steps:

1.A random number R is selected and is encrypted by making use of the public key K_S^{Pub} of the source agency. On target response, the encrypted random number R_V will be used to certify that the response corresponds to the apposite source request.

$$R_V = Enc[R]_{K_S^{Pub}}$$

2.A set of random values S_R, the source agency identifier and the request are combined with the encrypted random number R_V to obtain SE_{Data}. The random values set S_R will be utilized to validate the identity of the target.

$$S_R = \{r_1, r_2, r_3, ..., r_n\}$$

$$SE_{Data} = R_V + src\ \ id + [S_R] + \mathrm{Re}\,quest$$

3.The MD5 Algorithm is employed to compute the hash value H_{val} of the SE_{Data}.

$$H_{val} = MD5[SE_{Data}]$$

4. The hash value H_{val}, set of random values S_R and the request are combined and encrypted with the private key $K_S^{\Pr i}$ of the source agency to form SA_{Data}. The encryption with the source private key validly authenticates the source's request.

$$S_{Data} = S_R + \mathrm{Re}\,quest + H_{val}$$

$$SA_{Data} = Enc[S_{Data}]_{K_S^{\Pr i}}$$

5. The encrypted random number R_V and the source agency identifier are then appended to SA_{Data} to form the user request $S_{\mathrm{Re}q}$. Eventually, the user request is encrypted with the public key K_T^{Pub} of the target agency to form $S_{\mathrm{Re}q}$.

$$S_{\mathrm{Re}q} = Enc[R_V + src\ \ id + SA_{Data}]_{K_T^{Pub}}$$

The framed source agency request $S_{\mathrm{Re}q}$ possesses the encrypted random number R_V, the source agency identifier $src\ \ id$, SA_{Data}, all encrypted with the target's public key K_T^{Pub}. Now, this source agency's request $S_{\mathrm{Re}q}$ is transmitted to the target intelligence agency. The block diagram in Fig 1 portrays the steps involved in structuring the source agency's request.

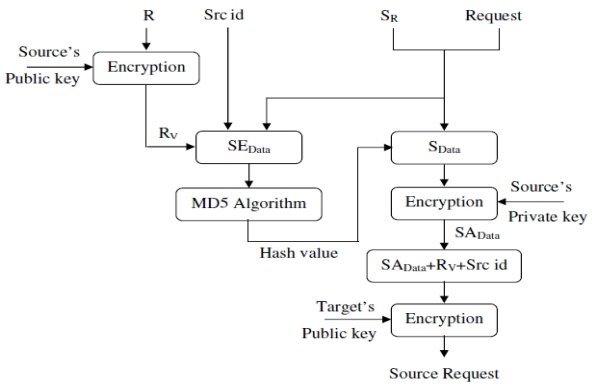

Fig .1: The structuring of source request

B. Steps in the Protocol at Target Agency

1) Validation of the Source Request

On receiving source agency's request, the target agency must authenticate source agency followed by validating the integrity of source agency's request. Then, on the basis of the trust level maintained with source agency, the target presents with an apposite and confidential response to the source

agency. The steps involved in the integrity checking and authentication of source agency's request are as follows:

1. The request $S_{\mathrm{Re}q}$ is decrypted with the private key of the target K_T^{pri}. As the private key is the secret property of the intended target agency, the target is assured that no one else can decrypt the request.

$$D_{\mathrm{Re}q} = Dec(S_{\mathrm{Re}q})_{K_T^{Pri}}$$

2. The $D_{\mathrm{Re}q}$ obtained from step 1 contains SA_{Data}, R_V and $src\ id$. The SA_{Data} obtained is decrypted with the public key K_S^{Pub} of the source agency. This authenticates that the request has originated from the claimed source agency.

$$D'_{\mathrm{Re}q} = Dec(SA_{Data})_{K_S^{Pub}}$$

$D'_{\mathrm{Re}q}$ contains the set of random numbers $[S_R]$, the request and the hash value H_{val}.

3. The SE_{Data} = ($R_V + src\ id + [S_R] + \mathrm{Re}quest$) is formed and its hash value $\overline{H_{val}}$ is computed with the aid of the MD5 algorithm. .

$$\overline{H_{val}} = MD5[SE_{Data}]$$

4. If the hash value computed from the above step and the hash value present in the source agency's request are identical, it ensures that the request has not been tampered during data transmission.

if ($H_{val} == \overline{H_{val}}$) *then*

request is not tampered

end if

The decrypted source request contains the encrypted random number, the source agency identifier, the set of random values and the request. The target agency's response is on the basis of the trust level maintained between the source and target agency, which is maintained in a database. The credibility and amount of information conveyed in the response depends on the trust level maintained with the communicating source agency. The block diagram in Fig 2 depicts the steps involved in the validation of the source agency's request.

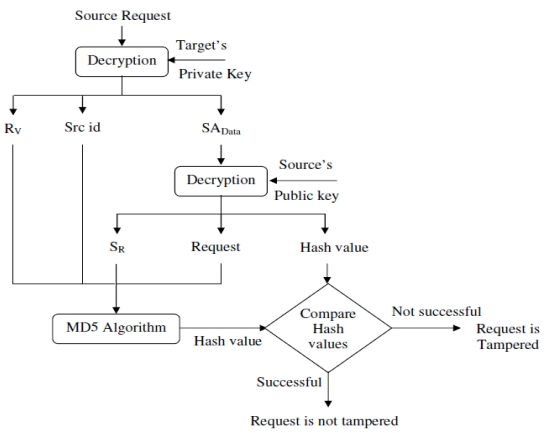

Fig. 2: Validation of the source request

2) Structuring of Response

The response to the corresponding source agency's request will be crafted as follows:

1. The target agency's database is scanned to attain the trust level maintained with the source agency. The trust level is a symbolization of the understanding levels of their respective countries. The source agency identifier serves as an index for the database search.
2. The encrypted random number R_V in the source request is kept as such in the response.
3. A mapping function M_{fn}, uniquely defined between the communicating agencies is retrieved from the target database based on the source agency identifier. It is then applied to the set of random numbers in the source request to attain a mapping value M_{val}. Subsequently, its sine value is computed and denoted as M'_{val}.

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

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

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

4. The target agency determines the amount and credibility of confidential information to be shared with the source agency based on the trust level obtained from Step (1).
5. The equivalent response for the source request and the calculated mapping value are appended to the TE_{Data}.

$$TE_{Data} = [R_V + M'_{val} + \mathrm{Re}sponse]$$

6. The MD5 Algorithm is employed to compute the hash value of TE_{Data} and is combined with TE_{Data} to form the eventual response.

$$H_{val} = MD5[TE_{Data}]$$

7. The structured eventual response of the target is lastly encrypted with the public key of the source agency K_S^{Pub} to acquire $T_{\mathrm{Re}s}$. This ensures the confidentiality of the information shared.

$$T_{\mathrm{Re}s} = Enc[TE_{Data} + H_{val}]_{K_S^{Pub}}$$

Afterwards, the encrypted target response $T_{\mathrm{Re}s}$ is sent back to the corresponding source agency. The block diagram in Fig 3 illustrates the steps involved in structuring the target agency response based on trust level.

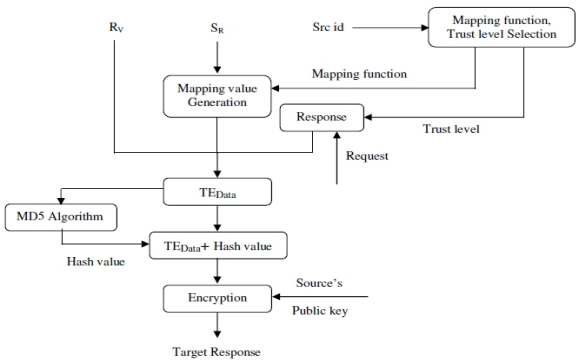

Fig. 3: Structuring of response

C. Steps in the Protocol at Source Agency

1) Validation of Target Response

On receiving the response from target, the source agency cannot deem it blindfold, but must make sure the following: 1) integrity of the target response 2) The response originated from the true or intended target (Authentication) and 3) The response corresponds to the apt request of the source agency.

1. The target response is decrypted using the private key of the source agency K_S^{Pri}, which discloses the encrypted random number, mapping value, the response and the hash value.

$$ST_{Res} = Dec(T_{Res})_{K_S^{Pri}}$$

$$ST_{Res} = [R_v + M'_{val} + \text{Re}\,sponse + H_{val}]$$

2. The response is confirmed for its integrity on the basis of the hash value computed using the MD5 algorithm.

$$\overline{H_{val}} = MD5[R_V + M'_{val} + \text{Re}\,sponse]$$

$$if\ \ (H_{val} == \overline{H_{val}})\ \ then$$

$$information\ \ is\ \ not\ tampered$$

$$end\ \ if$$

3. The mapping value present in the response is recomputed at the source agency to ensure that the response came from the intended target.

$$if\ \ (M'_{val} == \overline{M'_{val}})\ \ then$$

$$The\ target\ is\ valid$$

$$end\ \ if$$

4. The encrypted random number in the target response is decrypted with the private key of the source agency K_S^{Pri} to assure if it is a valid response for the request made.

$$if\ (R == Dec[R_V]_{K_S^{Pri}})$$

$$The\ response\ is\ valid$$

$$end\ if$$

5. After evaluating all these parameters, the source agency deems it as valid response from the target.

All the above steps guarantee that the proposed trust-based security protocol is effective in providing confidential, authenticated and secure information sharing. Further communications between the agencies follow the procedures discussed above. The block diagram in Fig 4 shows the steps involved in the validation of the response.

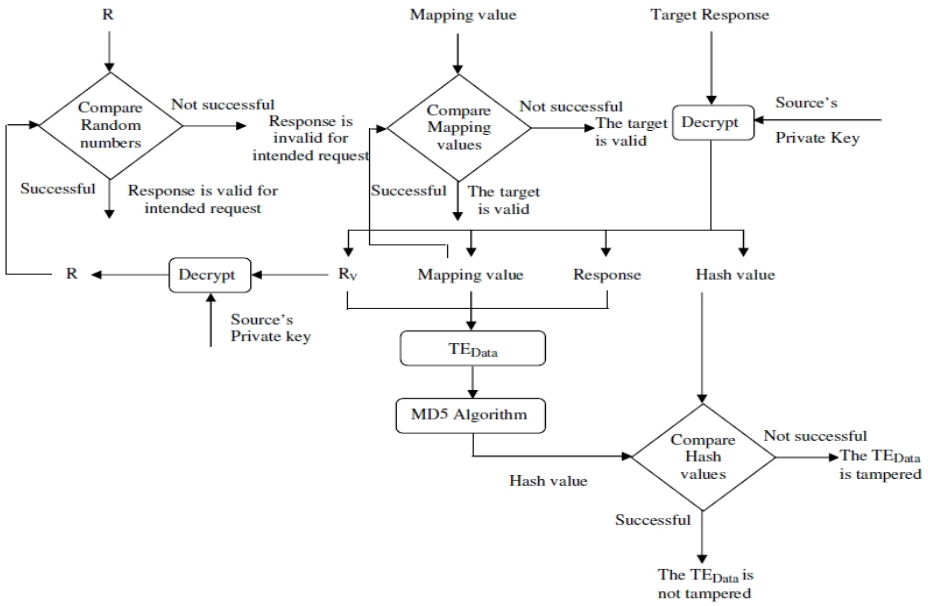

Fig. 4: Validation of the target's response

IV. EXPERIMENTAL RESULTS

The experimental results of the presented trust-based information sharing protocol are presented in this section. The proposed trust-based information sharing protocol is programmed in Java (JDK 1.6). The results acquired from experiments show that the presented protocol provides an effective and secure information sharing mechanism for communicating government intelligence agencies. The presented protocol is described as a three-way handshaking procedure to accomplish secure information sharing. The process started with a request for secret information about terrorists and their activities, by utilizing the techniques of hashing, a unique mapping function and public key cryptography. The target agency after a security verification responded with the suitable information on the basis of the trust level maintained with the source agency. The information shared will be a subset of the information available with the target agency based on the trust level. At the source agency, the legitimacy and confidentiality of the response is verified.

TABLE I: RESULTS OF EXPERIMENTATION

Source Agency	Target Agency	Terrorist ID	Information available with the Target agency	Trust-based Shared Information
CIA	FBI	98LetT8	{81,82,83,84,85,86,87,88,89,90}	{86,83,85,88,82,81,89,90,84}
ISI	CIA	98LetT8	{81,82,83,84,85,86,87,88,89,90}	{86,83,85,88,82,81,89,90,84}
RAW	CIA	03AlqT9	{91,92,93,94,95,96,97,98,99,100}	{97,94,98,95}
RAW	FBI	06TalT7	{71,72,73,74,75,76,77,78,79,80}	{79,72,76,74,78}
CIA	RAW	98LetT8	{81,82,83,84,85,86,87,88,89,90}	{86,83,85,88,82,81,89,90}
RAW	CIA	06TalT7	{71,72,73,74,75,76,77,78,79,80}	{79,72,76}
FBI	RAW	98LetT8	{81,82,83,84,85,86,87,88,89,90}	{86,83,85,88,82,81}
ISI	FBI	03AlqT9	{91,92,93,94,95,96,97,98,99,100}	{97,94,98,95,99}
CIA	FBI	06TalT7	{71,72,73,74,75,76,77,78,79,80}	{79,72,76,74}
ISI	FBI	98LetT8	{81,82,83,84,85,86,87,88,89,90}	{86,83,85,88,82,81,89,90}

Table 1 depicts the results obtained from the experimentation on the proposed trust-based security protocol using duplicate data. From the table, it is obvious that the quantity of information shared between communicating government intelligence agencies depends on the trust level maintained between them. In Table 1, the field "Information available in the target agency" gives complete security information available with the target intelligence agency about the terrorist and their suspicious activities, which has been collected over long periods of time and the field "Trust-based shared Information" consists of the information shared between the government intelligence agencies based on the trust level, without harming their own national interests. The experimental results portray that the presented trust-based security protocol enables effectual and secure information sharing on the basis of trust between global government intelligence agencies without affecting their own national interests.

V. CONCLUSION

Trust-based 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 article, we have presented an innovative, proficient and trust-based security protocol for confidential sharing of secret information amongst government intelligence agencies. The designed trust-based security protocol has offered confidentiality, authentication, integrity and agency verification by utilizing MD5 Algorithm, public key infrastructure and a unique mapping function. Also, on the basis of a predefined trust level, a restricted privacy is maintained between the communicating agencies. The proposed protocol will enhance the trust level between the communicating parties by enabling efficient and confidential sharing of secret information.

REFERENCES

[1] Al Sawafi.A, 2003. "E-Governance Technologies for enabling trust in Citizen Relation Management", In proceedings of *the Symposium on E-Government: Opportunities & Challenges*.

[2] Zhiyuan Fang, 2002. "E-Government in Digital Era: Concept, Practice, and Development", *International Journal of the Computer, the Internet and Management*, Vol 10, Issue 2, pp. 1-22.

[3] Anthony M. Cresswell, Theresa A. Pardo, Shahidul Hassan, 2007. "Assessing Capability for Justice Information Sharing", Proceedings of the *8th annual international conference on Digital government research: bridging disciplines & domains*, Vol 228, PP: 122-130.

[4] Seema Degwekar, Jeff DePree, Howard Beck, Carla. Thomas and Stanley Y. W. Su, 2007. "Event-triggered Data and Knowledge Sharing among Collaborating Government Organizations", Proceedings of *the 8th annual international conference on Digital government research: bridging disciplines & domains*, Vol 228, PP: 102-111.

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

[6] "A Blueprint for Better Government: The Information Sharing Imperative", NASCIO.

[7] Grosof, B.N., Feigenbaum, J., Li, N., 2003. "Delegation Logic: A Logic-Based Approach to Distributed Authorization". *ACM Transactions on Information and Systems Security*, Vol. 6, No. 1, pp 128-171.

[8] Seung-Yong Rho and Lung-Teng Hu, "Citizens Trust in Digital Government: Toward Citizen Relation Management", In proceedings of *2nd Annual Digital Government Research Conference*, Los Angeles, CA, May 2001.

[9] Athman Bouguettaya, 2004. "Enforcing Privacy in Next Generation Digital Government Applications", *CISC Research Report* 04-03.

[10] Theresa Pardo, 2002 "Realizing the Promise of Digital Government: It's more than Building a Web Site", *Information Impacts Magazine*, Vol 17, Issue 2.

[11] Violetta Cavalli-Sforza, Jaime G. Carbonell and Peter J. Jansen, 2004. "Developing Language Resources for a Transnational Digital Government System", *Language Technologies Institute*, Carnegie Mellon University, Pittsburgh, U.S.A, PP: 945-948.
[12] United Nations department economics and social affairs (Eds), 2007. "Managing Knowledge to Build Trust in Government", United Nations Public Administration Programme, PP: 28-46, New York.
[13] Hui-Feng Shih and Chang-Tsun Li, 2006. "Information Security Management in Digital Government", Encyclopedia of Digital Government, *Idea Group Publishing*, Vol. 3, pp. 1054 - 1057.
[14] Peng Liu and Amit Cheta.l, 2005. "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.
[15] Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.D., 1999. "The Keynote Trust-Management System", version 2, *IETF RFC* 2704.
[16] Chu, Y., Feigenbaum, J., LaMacchia, B., Resnick, P., Strauss, M., 1997. "REFEREE: Trust Management for Web Applications", *World Wide Web Journal*, Vol. 2, pages 706-734.
[17] Clarke, D., Elien, J., Ellison, C., Fredette, M., Morcos, A., Rivest, R.L, 2001. Certificate Chain Discovery in SPKI/SDSI. *Journal of Computer Security*, Vol. 9, No. 4, pp 285-322.
[18] Ignacio J., Michael E., Thomas E., Bradford J and Andrew.P, 2007. "Investigating the Dynamics of Trust in Government: Drivers and Effects of policy Initiatives and Government", In Proceedings of the *4th Workshop on Trust within and between organizations*, VU University, De Boelelaan.
[19] Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.D, 1996. "Decentralized Trust Management". In Proc. the 1996 *IEEE Symposium on Security and Privacy*, pages 164-173.
[20] Manisha Shekhar, 2009. "Crisis Management - A Case Study on Mumbai Terrorist Attack", *European Journal of Scientific Research*, Vol 27, Issue 3, PP: 358-371.
[21] Guido Bertucci, 2007. "Managing Knowledge To Build Trust In Government", United Nations Department of Economic and Social Affairs, *United Nations Publication*, New York.
[22] Xin Lu, 2007. "Distributed Secure Information Sharing Model for E-Government in China", *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Vol 3, PP: 958-962.
[23] Fillia Makedon, Calliope Sudborough, Beth Baiter, Grammati Pantziou and Marialena Conalis-Kontos, 2003. "A Safe Information Sharing Framework for E-Government Communication", *IT white paper from Boston University.*
[24] Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang, 2006. "Secure information sharing enabled by Trusted Computing and PEI models", Proceedings of the *ACM Symposium on Information, computer and communications security*, pp: 2 - 12.
[25] Jing Fan, Pengzhu Zhang, 2007. "A Conceptual Model for G2G Information Sharing in E-Government Environment", *6th Wuhan International Conference on E-Business*, Wuhan (CN).
[26] Theresa A. Pardo, 2006. "Collaboration and Information Sharing: Two Critical Capabilities for Government", Center for Technology in Government, *University at Albany Annual Report.*
[27] Theresa A. Pardo, J. Ramon Gil-Garcia, G. Brian Burke, 2006 "Building Response Capacity through Cross-boundary Information Sharing: The Critical Role of Trust", Paper presented at the *E-Challenges Conference*, Barcelona, Spain.
[28] Akhilesh Bajaj, Sudha Ram, 2003. "IAIS: A Methodology to Enable Inter-Agency Information Sharing in eGovernment", *Journal of Database Management*, vol: 14, no: 4, pp: 59-80.
[29] G. Beavers and H. Hexmoor, 2003. "Understanding Agent Trust", in Proceedings of the *International Conference on Artificial Intelligence* (IC-AI): 769-775.
[30] Golbeck, Jennifer, Bijan Parsia, James Hendler, 2003. "Trust Networks on the Semantic Web", Proceedings of *Cooperative Intelligent Agents*, Helsinki, Finland.
[31] Tryg Ager, Christopher Johnson, Jerry Kiernan, 2006. "Policy-Based Management and Sharing of Sensitive Information among Government Agencies," *MILCOM* 2006, pp: 1-9.
[32] Nabil R. Adam, Vijay Atluri, Soon Ae Chun, John Ellenberger, Basit Shafiq , Jaideep Vaidya, Hui Xiong, 2008. "Secure information sharing and analysis for effective emergency management", Proceedings of the *international conference on Digital government research*, Vol. 289, pp:407-408.
[33] Nabil Adam, Ahmet Kozanoglu, Aabhas Paliwal, Basit Shafiq, 2007. "Secure Information Sharing in a Virtual Multi-Agency Team Environment", *Electronic Notes in Theoretical Computer Science*, Vol: 179, pp: 97-109.
[34] Achille Fokoue, Mudhakar Srivatsa, Pankaj Rohatgi, Peter Wrobel, John Yesberg, 2009. "A decision support system for secure information sharing", Proceedings of the *14th ACM symposium on Access control models and technologies*, pp: 105-114.
[35] Md.Headayetullah and 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.

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, Allahabd, India in 2005. He was the topper of the University in his M.Tech Degree. He is currently pursuing the Ph.D (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, Bhubaneswar, India. He works in the field of E-Government, Digital Government, Networking, Internet Technology and Mobile Communication. He is currently working as an Assistant Professor in the Department of Computer Science & Engineering and Information Technology, Dr. B.C. Roy College of Engineering, Duragpur, West Bengal University of Technology, Kolkata, India.

G.K. Pradhan received the Ph.D degree from Indian Institute of Technology (IIT) Kanpur, India. He served as a lecturer, Assistant Professor and Associate Professor in various Institutes in India. Dr. Pradhan is currently working as a Professor & Head in the Department of Computer Science & Engineering and Information Technology, Institute of Technical Education & Research (Faculty of Engineering) of Siksha O Anusandhan University, 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 Ph.D degree in the field of Computer Science and Engineering and mathematics. His filed of interests are Software Engineering, E-Commerce, Digital Government, Internet Technology and Mobile Communication.