



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

An Enhanced PKI Based Information Sharing Security Protocol for Secure Digital Government and Mobile Government System

Dr.Md.Headayetullah¹, Dr. G.K. Pradhan², Dr. A. Anjum³

¹ Associate Professor, PG Department of Computer Science & Engineering, Bengal College of Engineering & Technology, Durgapur, West Bengal University of Technology, PhD (SOA University, Bhubaneswar), India

² Professor, PG Department of CSE/IT, SOAU, Bhubaneswar, PhD (IIT Kanpur), India

³ PG Department of Medical Science and IT, CMC, India

Abstract: Digital Government and Mobile Government are chiefly an issue of receiving public sector Information Technology schemes adapt to interoperability with citizen's digital government devices furthermore mobile devices. Enhanced interoperability involving public and private organizations is of key value to formulate digital government new-fangled victorious. Incidentally, expanding a sound digital government with mobile or digital government framework in the public sector is an imperative issue. Widespread digital governments with mobile public services framework must primary and leading amalgamate the following five principles: Interoperability, Security, Openness, Flexibility and Scalability. Digital Government security is precise one of the key aspect for pulling off an advanced stage of digital government along with mobile government. Digital government with mobile government must make sure security for its information systems, including computers and networks for providing better service to the citizens. Governments around the world are progressively more spinning to information sharing and integration, for solving problems in programs and policy areas. Harms of international agonize for example disorder discovery and run, terror campaign, colonization and border control, forbidden drug trafficking, and more demand information sharing, harmonization and cooperation amid government agencies within a country and athwart national borders. Countless disheartening challenges endure to the progress of an efficient information sharing protocol. A protected, trusted, role and cooperation based improved information-sharing protocol is required to enable mobile users or users to relate and share information easily and perfectly across many diverse networks, mobile devices and databases globally. This article chiefly presents (1) literature review of digital government security, mobile government, PKI based security approach and interoperability, (2) key research issues of mobile government, conceptual framework and adaptation mechanism and (3) an well-organized enhanced PKI based information sharing security protocol for secure exchange of top secret information amongst security personnels and government departments within the national boundaries under the digital and mobile government system. While trust-based, role and cooperation based information access is well studied in the literature, presented secure information sharing technologies and protocols cannot offer enough incentives for mobile or digital government agencies to share information amid them without harming their own national interest. To overwhelm the drawbacks of the accessible technology, a ground-breaking and talented enhanced security protocol is anticipated in this article for sharing of top secret information among government intelligence agencies internationally. The improved security protocol intended assures the enhanced interoperability of the digital and mobile government by sharing secure and updated information among government intelligence agencies to evade intimidating deeds. The experimental results exhibit the efficiency of the proposed PKI based information sharing security approach. In addition, this paper has shown, the citizens should be carefully educated in order to feel comfortable with mobile or digital government system. Key points of innovative ideas and views for further research and development in this field is first attempted in the paper.

Keywords: Digital Government, Interoperability, Information Sharing, Security, Trust, Public-Key Cryptosystem, Government Intelligence Department, Security Personnels, Message Digest 5 (MD5), ranking, Mobile Government, PKI.

I. Introduction

The terms "government" and "governance" are presently in extensive use, occasionally interchangeably. It is vital to build up a difference amongst two. Government is an institutional superstructure that society uses to transform politics into policies and legislation. Governments are precise institutions that incorporate to governance. Government is a user of information technologies, provider of information based services and major collector and purveyor of data and information [1]. Electronic Government (also known as e-Gov, digital government, online government or in a certain context transformational government) refers to government's use of information technology (IT) to exchange information and services with citizens, businesses, and other arms of government. E-Government may be applied by the legislature, judiciary, or administration, in order to improve internal efficiency, the delivery of public services, or better processes of democratic governance. 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 nurturing digital government, which is nothing but the usage of extensive applications of information and communication technology that handles every transaction of government services [3]. Digital government is typically term as the creation and transmittal of information and services within government and amongst government and the public by means of a range of information and communication technologies. The impact of digital government varies broadly across the world and is also known as e-government or virtual government [4]. E-government

services are established in a multifaceted architectural and technological scenario [5]. Information age technologies give huge opportunities for a government to transform its functions into the digital arena [6]. Many government agencies have adamantly engaged information technologies for updating the government's tremendously disjointed 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 fashionable uprising in information resulted on organizations within the entire world to greatly count on enormous numbers of databases to accomplish 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, inspection notes, scientific facts, commercial transaction data, and other. Information changes in the level of detail, the quantity or type of data exchanged. Due to lack of standard methods for electronic government information sharing, the means of sharing nowadays are not equally scrutinized, above-board and documentation [10]. The information sharing environment is complex and modern resolutions and partnerships are essential to accumulate shared benefits [11]. Additionally, the sharing is not continually guaranteed to be harmless from risks that might hold unlawful access, malicious amendment, and demolition of information or misinformation, computer intrusion, copyright infringement, privacy contraventions, human rights violations and more [10]. Since government departments are in necessitate sharing information inside the identical government and also transversely governments, the work out of a successful security determine is crucial. At a halt, a department cannot randomly let slip its database to any another departments [25, 27]. There are also several technology-specific sub-categories of electronic government, such as mobile government (m-Government), ubiquitous government (u-Government), and g-Government (GIS/GPS applications for e-Government).

E-Government is the exercise of information and communication technologies (ICTs) to advance the tricks of public sector organization. In the case of m-government, those ICTs are restricted to mobile and/or wireless technologies like cellular/mobile phones, and laptops and personal digital assistants connected to wireless local area networks. M-Government can aid to build public information and government services accessible "anytime, anywhere" to citizens and officials. M-Government should not be seen as something newest: for instance, wireless technology has always been an imperative part of law enforcement [36].

Only nowadays, police officers are as apt to employ a laptop wirelessly associated to the Internet as the good old two-way radio. When officers mark a mistrustful vehicle they can straightforwardly search databases that present information on who owns the vehicle, if it has been reported stolen or else has been reported at a crime prospect, and if the owner is wanted by police or has jumped bail. Health and safety inspectors can now file their reports from the field in actual time using a Pocket PC or handheld terminals, reducing paper forms and the necessitate to re-enter the data collected when they get back to the office [37].

A sheltered and trusted information-sharing atmosphere is a prerequisite to facilitate users to communicate with and share information devoid of intricacy and immaculately across countless divergent networks and databases universally. This means can significantly move forward the effectiveness of plentiful functions, for example intelligence assembly and public safety hard work [22, 26, 28, 18]. Guarantying safety measures for its information systems, collectively with computers and networks, is a basic prerequisite for a digital government to function to the anticipation of its people. Information security is nothing but defending information and information systems from unconstitutional access, use, disclosure, disruption, modification, or destruction. The crucial elements of information security encompass integrity, confidentiality, availability, authentication that has to be well thought-out at various levels inside the hierarchy [23]. Production of an extensive basement for information sharing desires trust among all information sharing partners. Insufficiency of trust cause fears that mutual information will not be protected recurrently or used appropriately; and, that sharing will not relentlessly happen in both directions [24]. By using a secure information sharing system, organizations can contribute with pledge in communities of trust ever since for this ground they have the power in an attempt to exactly preside over their information right to use and practice.

Let us deem a local law enforcement officer at a usual traffic stop. Basic protocol sheers that the officer appeal and verify the individual's driving license and vehicle registration. At a standstill, the officer might in count confirm a wide assortment of other computer applications, for example colonization databases, terrorist watch lists, criminal information and intelligence repositories, and counter-drug intelligence databases that may be hold by external organizations, for example the U.S. Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Homeland Security. To implement this, these superficially owned applications have to be capable to identify the officer so as to decide if he or she has the precise credentials to obtain the information. Subsequently, the information that is accountable to be thin-skinned from an intelligence and privacy viewpoint is ought to be cosseted whilst in shipment. Finally, the device on which the officer assembles the information should be accomplished of storing that information firmly [12]. In our former works, we have proposed efficient and secure information sharing protocols for secure exchange of confidential information amongst government intelligence agencies [29, 30, 58, 59]. This paper is advanced edition of our aforementioned research article [59].

In this paper, we present an effective enhanced PKI based information sharing security protocol for sharing top secret information among the various government departments and security personnels of digital (or mobile) government system. The proposed protocol is predominantly adapted to fit in the subsequent circumstances. Consider, for instance, a local law enforcement officer at a usual traffic stop. The standard protocol for traffic control demands the officer to request and confirm the individual's driving license and vehicle registration. However, the law enforcement officer could also desire to check with an widespread range of other computer applications, such as colonization databases, criminal information and intelligence repositories, and counter-drug intelligence databases that may be possessed by external organizations, for example Central Bureau of Investigation (CBI), the Drug Enforcement Administration, and the Department of Homeland Security. The exactness and the sum of information shared amid security personnel and corresponding government intelligence departments is based on the predefined ranking of the security personnels. The wished-for effective trust, responsibility and teamwork PKI based information sharing protocol does well 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 fundamental sketch out of the paper is as follows: A brief appraisal of some modern researches related to the interoperability, mobile government, digital government and the improved wished-for secure security approach is given in Part II. The vital problem, issues, conceptual framework and adaptation mechanism of mobile government are presented in Part III. An enhanced PKI based information sharing security protocol for security personnels to share secure information among the government departments in mobile or digital government system are presented in Part IV. The experimental results are presented in Part V. Finally, the summary and concluding remarks are summed up in Part VI. In this section scholar and practitioners can able to identify an innovative position and prepare for future development for interoperability, security and implementation mechanism of mobile or digital system in digital government research.

II. Review of Related Research

The development of prospective maturity model of digital government interoperability is one of the leading research areas. Since the information sharing is the key to victory of digital government interoperability. Therefore, a plentiful of information sharing protocols has been proposed by researchers for efficient information sharing stuck between communicating parties and to deal effective interoperability amongst the digital government agencies. Digital government interoperability can be reached by sharing and amalgamating top secret information among the communicating parties. As a result, the development of trust-based secure information sharing protocols is as well one of the key issues for arrangement of digital government and mobile government interoperability. Lately, rising efficient approaches for securely sharing secret information amid government agencies and departments has careworn greatly concentration. A brief review of some latest researches is presented at this time.

Papazoglou *et al.* [39] have wished-for interoperability standards. The propose standards require consistency in four dimensions: (i) technology, (ii) syntax, (iii) semantics, and (iv) pragmatics. Technology standards disquiet middleware, network protocols, security protocols, and the like. Syntax standardization means that the network organization has to agree on how to integrate assorted applications based on the structure or language of the messages swapped over. In general, normally appropriate data structures are designated to suggest distinguished constructs. Semantic standards encompass agreements in additional room to syntactic agreements on the meanings of the terms used for an enterprise's information systems. Pragmatic standards are agreements on practices and protocols triggered by unambiguous messages, for example orders and delivery notifications. They also proposed innovative e-business models to diminish costs and enhancement of digital government internal and external operations foremost services. This proposed model supports citizen-centric services by integrating and sharing information among the stakeholders together vertically and horizontally. Pardo *et al.* [43] have offered digital government perception as well information sharing process. In accordance with Pardo, digital government, e-Government, and e-governance are terms that have become indistinguishable with the use of information and communication technologies (ICT) in government agencies. Inter-organizational information integration has become a key enabler for digital government. The wished-for article depicted two complex information sharing process for example: practical process and governmental process. In practical process the system designers and developers must frequently utilize over problem correlated to the survival of copious platforms, wide-ranging database designs and data structures, tremendously capricious data quality, and contradictory network infrastructure. In governmental observation, these practical processes recurrently utilize new work processes, mobilization of constrained assets, and developing inter-organizational interaction. The proposed articles present the crucial changes in societal communication for digital government information sharing process by taking into account of group decision-making, learning, perceptive, conflict resolution and trust building amongst government agencies. Trust based information sharing is further significant in digital government process.

Schooley *et al.* [40] have projected the recent line of digital government research concerning the worth of inter-organizational information sharing in the public province. They used a time-critical information services conceptual framework as analytical lens. The proposed inter-organizational system provided a targeted means to consider the cross-organizational features of a sociotechnical system. The projected system enhanced the

information sharing capabilities of diverse department of the digital government. The public sectors services can be enhanced by improving the information sharing among inter-organizational system such as: criminal justice, geographic and institutional boundaries. Fedorowicz *et al.* [41] proposed the concept of Inter-organizational system in which agency collaboration must be put up an extensive range of factors from the external environment and contributed organizations as component of their design and operation. They depicted the importance of the collaboration of the government agencies transversely jurisdictional and resourceful margins. Luna-Reyes *et al.* [42] illustrated various benefits of digital government by integrating the information diagonally organizational boundaries. They mugged the somber challenges as the required level of inter-organizational collaboration and trust was often not supported by exiting institutional agreements, organizational structures and management processes.

Scholl *et al.* [44] have offered E-Government or more suitably digital government interoperability and nine constraints. The offered constraints have subjective the integration and interoperability of digital government. Digital government interoperability is the technical ability for digital government interoperation. The wished-for nine constraints as follows: (1) Constitutional/legal constraints: Integration and interoperation may be uttered illicit because the democratic constitution requires powers to be estranged into separate levels and branches of government. The US constitution, such as, separates government into federal, state, and local government levels, and into legislative, judicial, and executive branches. Integral integration and interoperability connecting and amid branches and levels might offend constitutional checks and balances. On the contrary, the constitution also affords and sanctions integration and interoperation in assured limits. (2) Jurisdictional constraints: alongside under the constitution, governmental and non-governmental constituencies operate in parallel from each other and own their information and business processes, integration, interoperation, and information sharing cannot be obligatory on them. Reasonably, as an independent entity, each constituency's contribution in any interaction is amateur. However, using jurisdictional authority, the government entity can occupy in integration and interoperation with other entities. (3) Collaborative constraints: Organizations are assorted in terms of their character and willingness for cooperation and interoperation with others. Past knowledge, socio-political organization, and leadership style persuade the degree of willingness and proficiency of potential interoperation. In cases of complementary leadership styles, enough socio-political organization, and encouraging record skill, integration and interoperation might prosper. (4) Organizational constraints: In this constraint the integration and interoperation might hard to arrange as organizational processes and resources may differ among organization rapidly. At rest, it facilitates improved degrees of integration and interoperation as the organization supports its organizational view. (5) Informational constraints: Transactional information might be more liberally shared compared to strategic and organizational information. Information quality standards arise when information are collecting, integrating and sharing across numerous domains. At rest, information stewardship promotes the use of shared information, which in turn fosters stewardship for giving out information. (7) Managerial constraints: Interoperation suits really extra complicated the extra parties with sundry welfare and wishes become anxious. Thus, the needs of the related management task might exceed the management capability of interoperating partners. However, beside the ranks of shared interests, interoperation and integration can embarrass. (8) Cost constraints: Integration and interoperation amid varied constituencies might be limited to the lowest frequent denominator in terms of availability of funds: likewise, unexpected budget constraints might conceal serious challenges to permanent interoperation projects finally. Likewise, information-sharing initiatives have noticeably helped to manage costs. In the cost margins of the relevant partners, certain projects emerge to be sustainable. (9) Technological constraints: The heterogeneity of digital government policy and network capabilities might limit the interoperation of systems to relatively low standard. In contrast, a growing number of digital government information systems might attach to superior standards eventually, such that improved interoperation becomes possible. (10) Performance constraints: Whilst performance checks warn, the higher the number of interoperating partners, the lower is the generally system performance in provisions of response time. Hitherto, the highlight on prioritized needs might assist less but more successful interoperations. The offered article proposes how to get rid of these nine limitations of digital government or e-government interoperation. This proposed work will help to achieve digital (or electronic) government operations and services that are efficient, agile, citizen-centric, accountable, apparent and efficient. The integration of government information resources and processes, so the interoperation of autonomous information systems, is imperative to manage these objective. On the other hand, mainly integration and interoperation efforts ambush serious challenges and limits.

King *et al.* [45] projected stage of growth models which have been used in organizational research and management research. The offered model portrayed various phenomena such as organizational life cycle, product life cycle, biological growth etc. These models understood that conventional patterns exist in the growth stage of the organization such as the sales levels of the products and the growth of the living organisms. These offered stages are (1) sequential in nature (2) occur as a hierarchical development that is not simply reserved and (3) engage a broad range of organizational activities and structures. They projected and tested four stages among the multistage growth model. Frankfort *et al.* [46] projected stage of growth models by using yardstick variable which was in one- dimensional range. The size of yardstick variables can be achieved using Guttman scales. Guttman scaling is a cumulative scaling method founded on ordering theory that suggests a linear relationship squeeze in between the elements of a domain and the items on a test. Nolan [47] planned multistage models for

organizational assessment. The offered model was with six levels for Information Technology (IT) development in organizations, which later was extended to nine levels. Earl [48] suggested a stages-of-growth model for rising e-business which integrated: (a) external communication, (b) internal communication, (c) e-commerce, (d) e-business, (e) e-enterprise, and (f) transformation. Rao et al. [49] wished-for a maturity model for electronic commerce (E-Commerce) growth in small and medium sized enterprises. Gottschalk et al. [50] proposed maturity model in the area of knowledge management system for mapping crime in law enforcement. They offered afterward, maturity model for IT outsourcing relationships. The offered model recognized assured uniqueness so as to point up firms in varied stages of development. Kazanjian et al. [51] set up that a numeral of multistage models had been proposed which assumed that predictable patterns existed in the growth of organizations and that these patterns extensively spread as distinct time periods best thought of as stages. These models have diverse distinctive exceptionality. Stages can be provoked by the search for new growth opportunities or as a response to internal crises. Copious models recommend that organizations progress through stages while others argue that there may be copious paths during the stages. They used the concept of overriding problems to the stages of growth. Overriding problems demand that there is a pattern of key concern which firms face for each theorized development rank. In criminal organizations, for example, overriding problems can shift from need of skill to need of resources to need of approach connected with varied stage of development. They fall out that moreover flawlessly or openly, stages-of-growth models share a general basic logic. Organizations experience transformations in their devise distinctiveness which permits them to mug the novel responsibilities or problems elicited by growth. The problems, responsibilities, or environments may move away from model to model, but around all suggest that stages emerge in a well-defined order so that the key of one set of problems or responsibilities leads to the appearance of a new set of problems and responsibilities that the organization must undertake.

Chen et al. [52] have offered stages of development models of electronic (or digital) government. The improvement model of electronic or digital government provides the users' information and services in enormous degree of solidity diagonally plentiful dimensions of electronic or digital government. These models present that electronic or digital government capabilities begin reasonably and predominantly provide fixed, with no return information, but grow gradually more distinguished and add interactive and transactional capabilities. These models forecast a imperative string of electronic or digital government that includes horizontal and vertical incorporation and the progress of proper portals and flawless inter-organizational interactions. There were three different types of electronic or digital government development or maturity models such as: (a) First model displays a handful aspect, the policy, technology, data, and organizational concerns that must be unwavering for organizations to growth to higher levels of electronic or digital government development with an aid rise in benefits for equally government organizations and end-users. It is essential to have both higher levels technology and organizational density to accomplish more well-known levels of electronic or digital government. (b) Second model recognized the following four stages of electronic or digital government integration: (1) catalogue with online presence, catalogue presentation, and downloadable forms, (2) transaction with services and forms online, working database, and supporting online transactions, (3) vertical integration with local systems linked to higher levels systems and within related functionalities, and (4) horizontal integration with systems integrated across different functions and real one-stop shopping for citizens. (c) Third model stresses expanding levels of data integration mandatory for precise transformational electronic government, but counsels that such data integration hoists noteworthy confidentiality concerns when the data involves personally specialized information. It was remarked that these models demand, but only on occasion make open, that the obscurity of these assorted forms of integration have anticipated resulted in myriad organizations achievement the highest level of electronic or digital government development. Tryg Ager et al. [54] projected a set of policy-based technologies to lenience enhanced information sharing between government agencies lacking discusses information security or individual privacy. The approach incorporates: (1) fine-grained access controls that sustain turn down and filter semantics for complex policy condition approval; (2) a muggy strategy skill that supports consolidation of information from copious sources subject to the source's original revelation policies of each; (3) a curation organization that sanction agencies to pertain and arrange item-level safety classifications and exposé policies; (4) an auditing system that accounts for the curation history of each information item; and (5) a attribution auditing technique that traces information derivations over time to present delay in evaluating information worth. The final intend was to present a compass to tenacity extraordinary information sharing problems in government agencies and proffer direction for the improvement of prospect government information systems.

Md.Headayetullah et al. [38] have anticipated intangible growth ranks for idyllic interoperability and security in recent digital government. This paper considered the status of the highly developed art in the slice of attractive digital government interoperability and security by means of extensive models. Interoperability put forward to the work out of Information and Communication Technologies to silky the progress of the harmonization of work and information flow. Interoperability articulates to a property of special systems and organizations permitting them to work equally. This paper presented flawless interoperability. Flawless interoperability presents to the employ of computer-based tools to passive information swapped and the use of this historic information shared among varied and merely isolated organizations in a mutual competitive economic networked environment. Information sharing and integration are being experimental as the most ever

more accepted methodologies by governments in the region of the world, for working out problems in a broad range of programs and policy areas. Issues of worldwide concern for example disease detection and control, terrorism, immigration and border control, prohibited drug trafficking, and more demand information sharing, harmonization and collaboration among government agencies within a country and transversely national borders. The presented information exchanges are, hitherto, often unproductive and flawless. Advanced interoperability among public organizations and private organizations is of imperative implication to expertise digital government hottest defender. The offered model might be useful by public organizations to establish innovative development and future road for improved interoperability. This paper mainly presented the imperative issues of digital government such as security, information sharing protocol and ideal interoperability for achieving a sophisticated phase of modern digital government. This paper also projected the conceptual development levels for ideal interoperability and security in modern digital government. To address the information sharing issue among government agencies, Peng Liu *et al.* [13] have offered an resourceful interest-based trust model and an information sharing protocol, which is included a group of information sharing policies also information exchange and trust negotiation are interleaved and mutually dependent on each other. In addition, the emerging technology of XML Web Services was utilized during the accomplishment of the proposed protocol. The implementation was utterly consistent with the Federal Enterprise Architecture reference models and can be clearly incorporated within current E-Government systems.

Jing F. *et al.* [15] have projected a theoretical model for information sharing in an electronic government infrastructure. They established that the Government-Government (G2G) information sharing model will aid in giving knowledge for G2G information sharing and assist decision makers in formulating decisions concerning the partaking in G2G information sharing. The anticipated conceptual model was test out to realize the aspects influencing the involvement in an e-government information sharing and bring to light the conceptual model via case study beneath Chinese government system. Fillia Makedon *et al.* [14] have offered a negotiation-based sharing system called SCENS: Secure Content Exchange Negotiation System which was being created at Dartmouth College with the support of several 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 assorted information which is valid to various different domains. They represented that with sensitive and distributed information the government users can accomplish arrangement on the conditions of sharing through negotiation. Xin L. [16] has recognized a distributed information sharing model with looked into the technique standard support of the model. It was figured out that the outflow of dealing with government information exchange and cooperation among agencies will be reduced by a raise in the prospective and efficiency of agencies' collaboration down to the secure e-government information sharing clarification.

Nabil R. Adam *et al.* [17] have observed the demands in integration, aggregation and secure sharing information to help situation consciousness and response at the strategic level. On removal of data from various independent systems, the system filters, integrates, and proficiently predicts information requisite to obtain a common operational picture, by utilizing context-sensitive parameters. One substantial demand was to help out secure information sharing. Sharing of information prolong to be a major intricacy due to the data privacy and ownership concerns plus owing to a extensive range of security policies followed inside various government agencies. Nabil Adam *et al.* [18] have offered a two tier RBAC proceed to facilitate security and discriminative information sharing among virtual multi-agency response team (VMART) plus when there is need, it allows VMART expansion by permitting new-fangled collaborators (government agencies or NGOs). They also offered a coordinator web service for every member agency. The coordinator web service confines the responsibilities such as, authentication, information dissemination, information acquisition, role creation and enforcement of predefined access control policies. Understanding of secure, selective and fine-grained information sharing was accomplished by the encryption of XML documents in par with related XML schema defined RBAC policies. Achille Fokoue *et al.* [19] have established logic for risk optimized information sharing through rich security metadata and semantic knowledge-base that detains domain specific concepts and relationships. They set 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 excellently (iii) supports explanation for non-shareability; these explanation along with rich security metadata and domain ontology allows a sender to wisely execute transformation of information with the intention of sharing the transformed information with the addressee. Besides, they have explained a secure information sharing architecture with the help of a frequently accessible hybrid semantic reasoned and showed a number of descriptive cases that highlights the benefits of the method while different with usual methodologies. Ravi Sandhu *et al.* [20] have offered a way to share secure information easily through modern Trusted Computing (TC) technologies which is not obtainable with pre-Trusted Computing technology. They have configured the PEI framework i.e. policy, enforcement and implementation models, and demonstrated its applicability in inspecting the issue and generating solutions for it. The PEI framework enables the profound investigation of potential trusted computing applications for secure information sharing in the impending work. Trusted Computing applications excluding information sharing also are expected to be examined. A group of policy-based technologies to provide augmented information sharing amid government agencies devoid of moribund information security or person's privacy has been developed by Tryg Ager *et al.* [21]. The method covers: (1) fine-grained access controls which sustain deny and filter semantics for accomplishment of complex policy

conditions; (2) a oppressive policy ability that makes possible amalgamation of information from various resources conforming to each source's original admission 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 put forward maintain in assessments of information quality. The final aspiration was to facilitate a capacity to tenacity surprising information sharing issues in government agencies and proffer ways for the growth of future government information systems.

Gail-Joon Ahn *et al.* [31] have treated with the problem of supporting choosy information sharing while sinking the possibility of unlawful access. They have proposed system architecture by integrating a role-based delegation framework. Besides by executing a proof-of-concept, they have demonstrated the practicability of their framework. Mudhakar Srivatsa *et al.* [32] have presented a calculus approach for secure sharing of tactical information. Three operators: Γ , $+$ and $\cdot$ 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 $\cdot$ operators with the semantics of information transforms. To quantify the tightness of values estimates in the approach, they have developed tangible 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 offered a mechanism that enables the source organization to send content based on organization policy and requirements to another collaborating organization in such a way that it could be accessed only by a precise group of users performing a precise task or by all device members in the intention organization. They have talented this by providing a hardware-based root of trust for the master controller and organization devices developing trusted computing technology. Arazyan H. [54] has presented the definition and perspectives of Mobile Government. The presented paper described, the mobile government is a rising regulation with reference to the increase of advanced mobile and wireless communication technologies that would get better the Quality of Service (QoS) that government services offer to citizens. Lack of standards and optimized data exchange protocols in mobile and wireless atmospheres slow down the latent of mobile government.

III. Key Issues and Conceptual Framework of Mobile Government

A. Key Issues of Mobile Government

The possible of employing mobile and wireless technology in electronic government or digital government is noticeably known. Lallana [55] has identified several issues of mobile government. The present articles need to be tackled for extensive accomplishment of mobile government in the world wide. The present article describes the some key issues for implementing successful mobile government within the environment of digital government. These are as follows:

- a) Infrastructure development of mobile government mainly refers to the development of Information Technology infrastructure. The Information Technology infrastructure must be at an acceptable level.
- b) The physical infrastructure designates the technology, equipment, and network required for implementation of mobile government. Institutional arrangements and software that make m-government transactions possible are also very important.
- c) Mobile Payments infrastructures are crucial for the triumph of mobile government. A very foremost hindrance for customers to purchase online is a reaction of suspect in sending their credit card information over the mobile phone or the Internet. Numerous solutions for mobile payment still recommend a greater security that the wired systems [56].
- d) Privacy and Security are the imperative issue of mobile government. Citizens have an enormous anxiety about the privacy and security in mobile government. The universal issue is the convincement that their mobile phone numbers might be traced, when they send their judgments and inquiries to the government. The government must surmount the doubt, and guarantee mobile users that people's privacy is bubble-like and the information will not be advertised to third parties. Wireless networks are calmed well thought-out at risk because they use public airwaves to send signals. As a result of interception in all traffic on the Internet, there is a huge prospect for strangers to molest on wireless networks to lift important information and temper with documents and files [56].
- e) User friendly refers to the mobile users. The success of mobile government will rely on mostly the number of its users, the citizens. Governments necessitate to present easy access to mobile government information in substitute forms, possibly, using video and voice communications, so as to enhance citizen participation and provide citizen-oriented services [36].
- f) Legal issues - the many countries in the world wide have not thus far taken on the Law of Fair Mobile Information Practices. In some cases the current legislative does not recognize mobile documents and transactions at all. Therefore, legal issues are vital issues for implementation of victorious mobile government and to protect unwanted activities.
- g) Compatibility and interoperability are also important issue of mobile government. One of the technical difficulties might come to pass from compatibility of the mobile systems with the offered electronic government systems. This may obtain even more grave in the cases of government offices having legacy

systems which may not be simple to amalgamate. The answer lies in employing open systems using open not suitability standards.

B. Content and Presentation Management Issues of Mobile Government

Publishing web pages has developed from the prime function of a “Webmaster” to a distributed model where functional staffs that are straightforwardly responsible for the content are anticipated to post information. For agencies with strong web development policies and standards, this did not present a problem. For all the others it resulted in incoherent page design, usability and accessibility problems. Content Management Systems (CMS) helped determine this problem by adding a formal structure to the web publishing process and required agencies to adopt enterprise-wide web design standards. The greater part of CMS products do a superior job managing the presentation of information, providing the display in a typical web browser. Wireless devices do not use typical browsers, nor is there a single standard for all wireless devices. Wireless devices also have dissimilar display capabilities that are limited by display size, support for color and graphics. The other issue that needs to be tackled is the input capability of wireless devices, e.g., lack of a full keyboard, buttons, and pen-based. Some devices employ Wireless Application Protocol (WAP) and Wireless Markup Language (WML), and other technologies are used in specific devices (e.g., cHTML - Compact HTML used in I-Mode cell phones, HDML - Handheld Device Markup Language, Web Clippings - PalmVii, and xHTML- Extensible HTML). Whilst government organizations may approve a definite standard for mobile employees, citizen access to government information and services may require agencies to support multiple standards/technologies.

Extensible Markup Language (XML) - The key to presentation management may also make easy other electronic government initiatives, and that is in the use of the Extensible Markup Language (XML) and Extensible Style sheet Language (XSL). The use of both technologies permits information content to be formatted for specific wireless devices. The World Wide Web Consortium (W3C) has unconfined the XML Schema as a W3C Recommendation, demonstrating that the specification is stable and contributes to Web interoperability. The recommendation covers the following three parts: (a) Part0: Primer, at <http://www.w3.org/TR/2001/REC-xmlschema-0-20010502/> (b) Part1: Structures, at <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/> (c) Part2: Data types, at <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>. Simple Object Access Protocol (SOAP) - another technology that may make possible mobile government. A key is the Simple Object Access Protocol (SOAP). SOAP is a trivial protocol for the exchange of information in a decentralized, scattered environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for unfolding what is in a message and how to process it, a set of encoding rules for articulate instances of application-defined data types, and a convention for representing remote procedure calls and responses. The XML, XSL and SOAP infrastructure will also make easy applications communicating straight with each other over the Internet. Supplementary information is available at <http://www.w3.org/TR/SOAP>, and from the Organization for the Advancement of Structured Information Standards (OASIS), an international consortium that creates interoperable industry specifications based on public standards related to structured information processing, at <http://www.oasis-open.org>. Wireless Application Service Providers (WASPs) - some government entities may not have the technical staff to maintain the required programming and deployment to link applications to multiple types of wireless devices. This has resulted in a new-fangled kind of service providers that can cope and configure application content for a range of wireless devices. The WASPs host and manage wireless applications for a variety of devices and protocol languages. WASPs may provide a solution until wireless technologies become less complex and more standardized.

C. Conceptual Framework of Mobile Government

The fundamental notion for conceptual framework is principle-driven. At first, the business requirements are analyzed and based on this set of conceptual architecture principles is established for use in organization and technical section [57]. The Conceptual framework must make certain consistency among the requirements and the principles in order that the business requirements will be assembled by a solution that matches the principles, and that the appropriate principles are always grounded in business requirements. The conceptual framework principles are well-known in a multi-level hierarchy. The top level includes common, general principles that, among other things, reproduce the need for consistency crossways the public sector. The next level includes principles that generally try to optimize the IT solutions inside the focus of the mobile communication and technology. At the lowest level are principles heading for towards a specific system and standard or range of systems and standards in a given institution that offers the service.

The purpose of the universal conceptual framework principles is to make certain the honouring of the visions and objectives of the electronic government (or digital government) initiative in the area of mobile communications. A widespread mobile public services conceptual framework must essentially integrate the following five principles such as: (1) Interoperability (2) Security (3) Openness (4) Flexibility; (5) Scalability. Our suggestion of a service-oriented model stresses that interoperability is not just based on reading data on mobile devices from other systems, but that there must be functional consistency amid the systems.

(1) Interoperability is based on mutual agreements in which the rules for communication are defined for each novel system that is associated. This model workings fine jointly in principle and in practice where there are only some well-defined parties with precise, stable needs for exchanging data. If information is to be effortlessly

swapped over between authorities, it is required for the mobile systems to speak the same language. The center of interoperability is the prerequisite of common data models and common protocols for exchanging data. The protocols must support the data models by means of supposed metadata (i.e. information about data), which describes and defines data.

(2) The security functions are prepared in such a way that the business requirements for security (of both the civil service and citizens) can be conveyed to a level that is acceptable in the given application circumstances. The solution also has to be adaptable for any new-fangled requirements, without a large part of the prior investment in security becoming insignificant. In many situations, the requirement for security will be seen as inconsistent with, for instance, interoperability and openness. Now the information will be prearranged according to understanding and to grade access according to the needs of the given parties. (3) The openness of the system is measured on several levels such as: open standards, open interfaces, open specifications and open source codes. (4) Conceptual framework of mobile government generally is flexible in nature. In principle, public authorities should use open, formal standards, but where this is not possible or attractive, the advantages and disadvantages via open de facto standards should be measured. The architecture is visualized in a modular design where chief functionalities are developed disjointedly in modules that, when joint correctly, accomplish the whole ideal process.

(5) Scalability should be built into a system from the set up. It is significant to be capable to maintain both the functionality and efficiency of the solution if the need changes, for example in respect of user numbers, transaction volume or data quantity. Modularity and scalability must also concern the nature and scope of the work. The data exchange format is founded on the existing XML standard. The prospect work is concentrated on two sub-areas: (i) Standardization process is to identify standards in XML for exchanging data between public authorities and between public and private institutions over light data exchange format suitable for mobile communication networks. This engages novel optimized procedures for exchanging XML data in binary form. (ii) The info database is a database encloses information on the comfortable of public databases and information on how to access this data. As well this system is to act as an innovation directory when a mobile user enters in area where new-fangled service is offered.

D. Adaptation of Mobile Government in India (Case Study)

Mobile government development spotlights generally on infrastructures, together with mobile networks and applications. Once the obligatory infrastructures is developed and adequate mobile concreteness is reached, governments will have to arrangement with the more tricky task of regulating and developing legal facet of mobile applications and use of the mobile services. This is also the problem that governments face when implementing electronic government (or digital government). At this phase, roles of legal involvements in developing mobile market can be achieved to the front and will settle on further triumph of mobile government proposals. As in case of electronic (or digital) government, mobile government has its improvement stages: one way communication, interaction and transaction.

Docomo was resulted from Nippon Telegraph and Telephone (NTT) in August 1991 to take over the mobile cellular operations. It provides 2G Personal Digital Cellular (PDC) services on the 800 MHz band, and 3G FOMA W-CDMA (Freedom of Mobile Multimedia Access Wideband Code Division Multiple Access) services on the 2 GHz universal mobile telecommunications system (UMTS2100) and 800 MHz (UMTS800 (Band VI)) and 1700 MHz (UMTS1700 (Band IX)) bands, and 4G LTE services. Its businesses also incorporated Personal Handy-Phone System (PHS), paging, and satellite. Docomo finished offering a PHS service on January 7, 2008. In 1991, the second generation (2G) cellular technology was commenced in Finland by Radiolinja on the GSM standard, which flashed contest in the sector as the novel operators faced the in office 1G network operators. In 2001, the third generation (3G) was launched in Japan by NTT DoCoMo on the WCDMA standard. This was pursued by 3.5G, 3G+ or turbo 3G improvement based on the high-speed packet access (HSPA) family, permitting UMTS networks to have higher data transfer speeds and capacity. In 2009, it had become graspable that, sometime, 3G networks would be plagued by the enlargement of bandwidth-intensive applications like streaming media. Accordingly, the industry began looking to data-optimized 4th-generation technologies, with the promise of speed improvements up to 10-fold over existing 3G technologies. The first two commercially available technologies billed as 4G were the Wi-MAX standard (offered in the U.S. by Sprint) and the Long Term Evaluation standard, first offered in Scandinavia by TeliaSonera. Wi-MAX (Worldwide Interoperability for Microwave Access) is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the 2011 renew providing up to 1 Gbit/s for fixed stations.

Being at the formative years of mobile government implementation process, governments should take benefit of handy second generation (2G) networks and start providing straightforward informational and interactive services, for example providing concise information connecting to administrative procedures passing through Short Message Services (SMS). The evolution to the transactional stage and provision of value added public services, for example providing platforms for downloading and exchanging administrative forms of doing different administrative transactions requires employment of the next generation of mobile networks i.e. third generation (3G) networks that permit mobile users to access the Internet via high speed mobile connections.

Set up 3G networks is flattering a worldwide mobile trend; since May 2006, 196 cellular operators in 84 countries have commenced third generation (3G) networks. With the adoption of 3G services by citizens and

improvement of contents for mobile platforms by directorial agencies, governments can initiate providing more successful services at fewer costs. Thus, mobile government tactic founded on mobile infrastructures suggests more gradual development of mobile government services involving less initial investments, as much as it relies on obtainable mobile networks, which will be shortly, promoted to 3G networks by cellular operators. In India data entry associated to village information and facilities available in diverse villages are prepared at concerned Panchayats which sequentially is associated to a central server (available at District surrounding villages can have the mandatory information on a particular village on their Mobile phones from their houses exclusive of surfing the Internet for example 'ct' Collectorate Head Quarter or State Head quarter), by means of the wireless technology in exacting Mobile phones people reside in surrounding villages can have the obligatory information on a particular village on their Mobile phones from their houses without surfing the Internet.

Right now, the majority of the State Governments in India have executed Treasury Information System in either Client Server mode or Web Based (i.e. 3-Tier Architecture). Definite reports are also being produced as per the claim of the apprehensive Finance department either in off line approach or online approach lest the application software is Web Based. But nobody can realize the volume of immediate withdrawals being made from the creature Treasury using the said application. Now, this article can integrate the use of Mobile Technology to burst the immediate withdrawals being made from a particular Treasury in appearance of SMS (Short Messaging System). The flash, the amount of withdrawals being made is more than a definite cut off amount as fixed by Finance Department, the apprehensive authority of finance department will obtain a SMS concerning the withdrawals being made who in order can make an enquiry at the same moment of time if required. This may confirm to be a better live paradigm which transforms a Government from electronic (or digital) government to Mobile government. This example is before now in place in the State of Haryana in India where the farmers are equipped knowing the price of different commodities on Mobile, transforming the government system to mobile government. Currently, in India every villager are well aware with the use of mobile phones rather than surfing Internet, the literacy rate being low down in most of the villages of our country. Perceptibly the government can plan the shortfall in a mobile fashion as an alternative of meeting and planning in a closed-door room. Sooner or later individual can expect mobile government to overrule the electronic (or digital) government.

To present an apparent picture about the user's willingness to adopt the mobile government channels, the present article accomplished an electronic survey about the citizen's opinion in the Indian civilization. India is a developing country with standard IT infiltration and strong infiltration of mobile and wireless technologies.

Table 1: Electronic Survey advantages from Mobile government in India

Advantage	% participants
Better Information	40%
Save time	32%
Better communication	28%
Freedom	22%
Mobility	20%
Democracy	20%
Transparency	15%
Save money	7%

The electronic survey was anonymous. The survey was proposed mainly for the employees and the student at the Bengal College of Engineering & Technology under West Bengal University of Technology in Kolkata, India. Total of 103 participants responded the questions in the electronic survey, 65% males and 35% females. The participants were chiefly immature people, in the age group 22-37 years old with well-built IT awareness. In proportion to the results, the key parts of the participants were not educated about electronic (or digital) government (65%) and especially 67% did not have an apparent portrait what is mobile government. From the remains, 57% maxim mobile government as a count to electronic (or digital) government and 43% measured them totally assorted. The participants figured numerous issues as advantages from executing mobile government services in India.

The typically tackled issues are offered in Table 1. Whilst it revives the State's plan about executing mobile government services, the participants clearly recognized that it should engage lead assignments, accomplishment of reasonable services with democracy/cost and services that are cost-effective in scenery. Finally, the partakers pointed out that the issues as: lack of knowledge in the government, lack of technical infrastructure, lack of initiative and extant of ministry of information technology should be considered as chief hindrance when implementing mobile government services in India. The verity that in India there are above 55% mobile phone users and the number of Internet users is slightly above 15% is substantial to conclude that in order to bridge the digital divide; the mobile government policy is must for a rising country as India. The critical number above 20% is reached and the technology infrastructure exists.

IV. Enhanced PKI Based Information Sharing Security Protocol for Security Personnels

Governments must keep in trust in the vital asset, government information and manage it proficiently. A greater fondness must be given by government organizations at all levels for the swap over information and data stuck

between and amidst its trusted partners. Information must be leveraged and sustain by harmonized and integrated solutions in order to accumulate the increasing needs and service requirements. The present “stove piped” environment has mired 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. Although the fact that some upgrading has been made, to identify how information sharing responsibilities and relationships, including proper central encouragement will progress this task, more activities are needed [6]. Building secure information sharing mechanisms for security personnels is not minor because security personnels fret that their interests may be imperil when they share information with government departments that are commerce with security [22]. The chief motivation behind this research is the design of an efficient and secure information sharing approach for strongly exchanging confidential and top secret information among security personnels and government intelligence departments.

This section describes the PKI based information sharing security protocol premeditated for secure exchange of secret information among security personnels and government intelligence agencies. Even though the anticipated security protocol is non-privacy-preserving, it assurances utmost confidentiality and authentication in information transfer for both the security personnel and the target government sections. In general, the security personnels get hold of secret information about mistrustful 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 crucial issue. This demands a well-organized trusted and mutual enhanced security protocol that offers confidential and authenticated information sharing without creating any issues and problems to the security section of the government. Moreover, there is a chance that the target government section may provide entire confidential information about a person to every the security personnels, which would disquiet the privacy of that person and leads to information leakage. The above case cannot be utterly avoid in a non privacy-preserving security protocol but could be restricted by allowing information transfer based on the security personnel’s ranking.

In the offered improved security protocol, the reliability of information shared is based on the ranking of the security personnel. A master control is established in the anticipated approach to inspect and control the information exchange sandwiched between the security personnel and the government intelligence sections. The projected trusted, secure and cooperative information sharing security protocol requires the following: (a) The public key of the security personnel, the master control and the communicating sections (b) A unique and complex mapping function to exceptionally identify the security personnels, the master control and the communicating intelligence section. The security personnels, the master control and the communicating government intelligence sections accomplish their public and private keys from a trusted Certificate Authority (CA). The key ladders concerned in the proposed enhanced information sharing security protocol are offered in the following stepladder.

A. Stepladder in the wished-for enhanced security protocol at the security personnel section

1) Arrangement of the security personnel’s query

The security personnel send request or query through mobile government or digital government for various secret information about vulnerable persons and their distrustful activities to the government intelligence sections. It is the duty of the security personnel to pass on the request or message in an indecipherable probably encrypted approach such that the hackers cannot extort any precious information or revise the information in the request. The arrangement of the security personnel’s request entails the following ladder:

1. A random number RVN is designated and encrypted using the security personnel’s public key K_{Se}^{Public} .

This encrypted random number E_{RVN} will be used to validate if the response corresponds to the appropriate security personnel’s request. $E_{RVN} = Enc[RVN]_{K_{Se}^{Public}}$

2. Subsequently, a set of random values R_v are chosen and they are combine with the encrypted random number E_{RVN} and the request to attain the source encrypted data SE_{Data} . The random values set R_v will be employed in the justification of the identity of the target government section. $R_v = \{r_1, r_2, r_3, \dots, r_n\}$;

$$SE_{Data} = [E_{RVN} + R_v + SPQuery]$$

3. With the help of the MD5 Algorithm, the hash value H_v is worked out from the source encrypted data

$$SE_{Data} \cdot H_v = MD5[SE_{Data}]$$

4. The security personnel’s request or query $SPQuery$ is then encrypted with the target government section’s public key to circumvent others from hacking or altering the request. Since the request is encrypted with the target section’s public key, it can be decrypted and sighted only by the target section.

$$S_{SPQuery} = Enc[SPQuery]_{K_{TR}^{Public}}$$

5. The hash value H_v , the set of random values R_v and the encrypted request or query $S_{SPQuery}$ are combined and encrypted with the security personnel's private key $K_{Se}^{Private}$ to obtain SA_{Data} . The encryption with the security personnel's private key authentically validates the security personnel's request.

$$SA_{Data} = Enc \left[R_v + S_{SPQuery} + H_v \right]_{K_{Se}^{Private}}$$

6. The encrypted random number E_{RVN} and the obtained SA_{Data} are combined and encrypted with the public key K_{MC}^{Public} of the master control to form the security personnel's request or message SP_{msg}

$$SP_{msg} = Enc \left[E_{RVN} + SA_{Data} \right]_{K_{MC}^{Public}}$$

The well thought-out security personnels' request or message SP_{msg} contains the encrypted random number E_{RVN} , and the obtained SA_{Data} , all encrypted with the master control's public key K_{MC}^{Public} . Currently, this structured request SP_{msg} is put out to the master control.

B. Stepladder in the wished-for enhanced security protocol at the Master Control (MC)

1) Validation of the security personnel's request or message

In receipt of the request or message from the security personnel, the master control must validate the security personnel followed by authenticating the integrity of the security personnel's message. Subsequently, the master control will append its identity to the request and send the same to the target government section. The ladder concerned in the integrity checking and authentication of the security personnel's request or message are as follows:

1. The request from the security personnel SP_{msg} is first decrypted using the master control's private key $K_{MC}^{Private}$. As the security personnel's original message is encrypted with the public key of the target government section, it couldn't be sighted by the master control. Since the private key is the secret possessions of the estimated target, the target is guaranteed that no one else can decrypt the request.

$$SMC_{msg} = Dec \left[SP_{msg} \right]_{K_{MC}^{Private}}$$

2. The SMC_{msg} obtained from the above step contains SA_{Data} and E_{RVN} . The SA_{Data} is then decrypted with the public key K_{Se}^{Public} of the security personnel. The victorious decryption authenticates that the request has invented from the alleged security personnel.

$$SMC'_{msg} = Dec \left[SA_{Data} \right]_{K_{Se}^{Public}} ; SA_{Data} = \left[E_{RVN} + R_v + S_{SPQuery} + H_v \right]$$

The SMC'_{msg} contains the set of random values R_v , the encrypted random number E_{RVN} , the encrypted request $S_{SPQuery}$ and the hash value H_v .

3. Next, the set of random values R_v , the encrypted request $S_{SPQuery}$ and the hash value H_v are combined and encrypted using the master control's private key $K_{MC}^{Private}$ to obtain $MC_{Request}$.

$$MC_{Request} = Enc \left[R_v + S_{SPQuery} + H_v \right]_{K_{MC}^{Private}}$$

4. Consequently, the master control forms $MC'_{Request}$ by amalgamating the encrypted random number E_{RVN} and the formed $MC_{Request}$ and then encrypting them with the public key of the target section K_R^{Public} . To finish, the formed MC'_{Req} will be sent to the target section. $MC'_{Request} = Enc \left[E_{RVN} + MC_{Request} \right]_{K_R^{Public}}$

C. Stepladder in the wished-for security protocol at the Target Section

1) Validation of the request or message by the Target Section

Subsequent to receipt of the security personnel's request or message from the master control, the target section must validate the master control and the security personnel followed by confirming the integrity of the security personnel's request or message. The ladders concerned in the above methods are as follows:

1. The request $MC'_{Request}$ received from the master control is earliest decrypted with the private key of the target section to obtain TR_{msg} . The TR_{msg} consists of the encrypted random number E_{RVN} and the $MC_{Request}$.

$$TR_{msg} = Dec[MC'_{Request}]_{K_{TR}^{private}} ; TR_{msg} = E_{RVN} + MC_{Request}$$

2. Subsequently, the $MC_{Request}$ is decrypted with the public key of the master control to obtain TR'_{msg} . The TR'_{msg} contains the set of random values R_v , the encrypted request $S_{SPQuery}$ and the hash value H_v .

$$TR'_{msg} = Dec[MC_{Request}]_{K_{MC}^{Public}} ; TR'_{msg} = R_v + S_{SPQuery} + H_v$$

3. Afterward, the authentic query or message from the security personnel $S_{SPQuery}$ is decrypted with the target section's private key, as $S_{SPQuery}$ is encrypted with the public key of the target section.

$$TR''_{msg} = Dec[S_{SPQuery}]_{K_{TR}^{Private}}$$

4. Next, the set of random values R_v , the authentic query TR''_{msg} and the encrypted random number E_{RVN} are combined and their hash value $\overline{H_v}$ is computed with the aid of the MD5 algorithm.

$$\overline{H_v} = MD5[E_{RVN} + R_v + TR'_{msg}]$$

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 or query are alike, it pledges that the request or query has not been altered during the transfer.

If $H_v = \overline{H_v}$ then
 SPQuery is not altered
 else
 SPQuery is altered
 end if

2) Arrangement of response or reply to the Security Personnel's request or query

Subsequent to triumphant validation of the security personnel's request, the target section will form response for the security personnel's query. The ladders concerned in formation the response are as follows:

1. The target section's database is scrutinized formerly to achieve the ranking of the security personnel, from whom the request invented. The ranking denotes the grade of security personnel, and it decides the sincerity of the information that must be given to the security personnel.

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

3. A mapping function $M_{function}$ distinctively defined stuck between the communicating parties is recovered from the target section's database. Apiece security personnel, there is a distinctive mapping function in the target section's database. Next, the acquired mapping function is applied on the set of random values R_v in the security personnel's request to attain mapping value M_{value} . Afterward, its sine value is computed and represented as M'_{value} . $M_{value} = M_{function}(R_v)$; $M'_{value} = Sin(M_{value})$ Where $R_v = \{r_1, r_2, r_3, \dots, r_n\}$, $M_{function} = \{+, -, *, /\}$

4. Subsequently, the target section establishes the amount and sincerity of secret information to be shared with the security personnel on the basis of the security personnel's grade obtained from steps 1.

5. The response match to the security personnel's request; the premeditated mapping value and the encrypted random number E_{RVN} are combined to form target encrypted data TRE_{Data} .

$$TRE_{Data} = [E_{RVN} + M'_{value} + Re ply]$$

6. With the aid of the MD5 Algorithm, the hash value H_v is calculated from the target encrypted data

$$TRE_{Data} . H_v = MD5[TRE_{Data}]$$

7. The response matches to the security personnel's request is then encrypted with the public key of the security personnel K_{Se}^{Public} , so that it can only be viewed by the security personnel. $S_{Re ply} = Enc[Reply]_{K_{Se}^{Public}}$

8. The encrypted response or reply $S_{Re ply}$, the encrypted random number E_{RVN} , the mapping value M'_{value} and the hash value H_v are combined and encrypted with the master control's public key K_{MC}^{Public} to form target response $TR_{Response}$. To finish, the formed $TR_{Response}$ will be sent to the master control.

$$TR_{Response} = Enc[E_{RVN} + M'_{value} + S_{Reply} + H_v]_{K_{MC}^{Public}}$$

D. Stepladder in the wished-for security protocol at the Master Control

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

In receipt of response from the target section, the master control must confirm the following: (1) integrity of the target section's response (2) The response invented from the proper or estimated target (validation). The ladders concerned in the above processes are as follows:

1. The target section's response $TR_{Response}$ is earliest decrypted with the master control's private key $K_{MC}^{Private}$, which discloses the encrypted random number E_{RVN} , mapping value M'_{value} , the encrypted response S_{Reply} and the hash value H_v . $TRC_{msg} = Dec[TR_{Response}]_{K_{MC}^{Private}}$; $TRC_{msg} = E_{RVN} + M'_{value} + S_{Reply} + H_v$
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 anticipated target section.

If $M'_{value} = \overline{M'_{value}}$ then The intended target is valid and forward the response ; else

Dispose of the response; end if

3. After the validation of the projected target, the encrypted response, the encrypted random number, mapping value and the hash value are united and encrypted with the public key of the security personnel K_{Se}^{Public} and is sent back to the security personnel. $MCS_{msg} = Enc[E_{RVN} + M'_{value} + S_{Reply} + H_v]_{K_{Se}^{Public}}$

E. Steps in the wished-for approach at the security personnel side

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

On being paid of the response from the master control, the security personnel must make sure the following: (1) integrity of the target section's response (2) The response created from the anticipated target (certification). (3) The response corresponds to the right request of the security personnel. The ladders concerned in the above processes are as follows:

1. The received response MCS_{msg} is foremost decrypted with the security personnel's private key $K_{Se}^{Private}$.

$$S_{Response} = Dec[MCS_{msg}]_{K_{Se}^{Private}}$$

2. The response is established for its integrity by computing the hash value and comparing it with the hash value from the target section. $\overline{H_v} = MD5[E_{RVN} + M'_{value} + Re ply]$

If $H_v = \overline{H_v}$ then

information is not tampered or altered; else information is tampered or altered ; else if

3. The encrypted random number in the target section's response is decrypted with the private key of the security personnel $K_{Se}^{Private}$ to make sure that the response is legitimate for the request made.

$$if (RVN == Dec[E_{RVN}]_{K_{Se}^{Private}})$$

The response is valid or The response is according to the requirement of Security Personnel
end if

4. Once appraising all the parameters in the target section's response the security personnel considers it as a suitable response from the valid target section. The entire above ladders assurance that the proposed enhanced PKI based information sharing security protocol is proficient for sharing top secret, authenticated and protected information. Added communications among the security personnel and the government intelligence departments pursue the security protocol conversed above.

V. Experimental Results

The results acquired from the experimentation on the wished-for enhanced secure information sharing security protocol are presented in this section. The presented enhanced PKI based information sharing security protocol is programmed in Java (JDK 1.6). The results obtained from the experiments demonstrate that the offered security protocol provides proficient and secure information sharing for security personnels and the government intelligence sections. The master control initiated in the proposed security protocol improves the security of information sharing by monitoring and controlling the information swapped over between the security personnel and the government intelligence sections. The progression started with a request for confidential information about a person, by utilizing the techniques of hashing, a unique mapping function and public key cryptography (PKC). The master control (MC) supervised and restricted together the request and response from the security

personnel and the government intelligence section. The target section after a security confirmation responded with the suitable information on the basis of the ranking of the security personnel. The information shared will be a compartment of the information available with the target section based on the ranking of the security personnel. Below, Table 2 portrays the results obtained from the experimentation on the wished-for enhanced PKI based trusted, cooperative and secure information sharing security protocol using reproduction data. From the table 2, it is understandable that the amount of information shared between the communicating parties depends on the ranking of the security personnel. In Table 2, the field *presented information in intelligence section contains* the confidential information about the persons and their mistrustful activities, which has been collected over long periods of time and the field *ranking-based shared information* consists of the information shared stuck between the security personnel and the government intelligence sections without harming their own national interest. The proposed enhanced security protocol profitably conserved the privacy of the person whose information is swapped over among the communicating parties.

Table 2: Results of Experimentation

Security Personnel under Digital (or Mobile) government Environment	Government Intelligence Section (Digital or Mobile government Environment)	Distinctive Identifier (Validation)	Presented Information in Intelligence Section (Coded Form)	Ranking-based shared information (without harming any national interest)
Security Personnel1	Intelligence Bureau (IB)	2	{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}	{33,76,48,21,52,67}
Security Personnel1	Central Bureau of Investigation (CBI)	1	{39,33,46,56,74, 46,49,50,59, 14,6,18,29,43, 67,45,69,58,60}	{67,45,69,58,60}
Security Personnel1	Narcotics Control Bureau (NCB)	3	{39,35,42,57,65, 49,52,64,77,87,90, 78,64,59,73,75,68, 13,17,19,24,29}	{78,64,59,73,75, 68}
Security Personnel2	Central Bureau of Investigation (CBI)	3	{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}	{46,23,25,18,29,30}
Security Personnel2	Criminal Investigation Department (CID)	1	{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}
Security Personnel3	Criminal Investigation Department (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 }
Security Personnel3	Intelligence Bureau (IB)	1	{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}
Security Personnel3	Narcotics Control Bureau (NCB)	2	{11,26,33,15,17,45, 13,17,18,28,24,32, 7,48,26,45,76,82, 37,21,28,17,19,25}	{11,26,33,15,17,45}
Security Personnel4	Central Bureau of Investigation (CBI)	1	{39,33,46,56,74, 46,49,50,59, 14,6,18,29,43, 67,45,69,58,60}	{14,6,18,29,43, 67,45,69,58,60}
Security Personnel4	Intelligence Bureau (IB)	2	{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}

VI. Summary and Concluding Remarks

The main advantage of mobile government over electronic government in rising and intermediary countries is that they have more highly developed mobile road and rail network than Internet support. Nevertheless, user-friendliness doesn't mean authentic use of services. General public can suspect mobile government services and transactions in anticipation of their privacy and security won't be guaranteed by government in the digital government environment. Legislation needs to be precisely developed to guarantee authenticity and legality of associated transactions, therefore encouraging wider service approval by citizens. Lack of standards and optimized data exchange protocols in mobile and wireless environment decelerate the latent of mobile government. Even though the recent mobile infrastructures and applications in the majority rising countries do not permit providing rational public services, but it does not mean there is a lack of applicable policy. The present article offers the key issues of mobile government and digital government, mechanism behind the adaptation of mobile government including case study in developing country like India and conceptual

framework of modern mobile government environment. Mobile government development spotlights generally on infrastructures, together with mobile networks and applications. These articles pointed out that the major issues as: lack of knowledge in the digital government, lack of technical infrastructure, lack of proposal and existing of ministry of information technology should be considered as chief impediment while put into practice mobile government services in rising country like India. Moreover this articles demands more sure information sharing services among general people, security personnel and government intelligence agency in the digital government environment as well as mobile government system. Therefore, this paper presents the blueprint, implementation and validation of PKI infrastructure that could be appropriate to any of government domain either digital or mobile. In this communications a set of trustful relationships is established to obtain a trustworthy model connecting general people, security personnel and government intelligence department of any country in the digital government and mobile government environment. Once these trust relationships have been created, certificates need to be defined with certain obligatory, required plus/otherwise optional expansions. Several comprehensible procedures moreover necessitate to be defined for building and validating certification pathways. Information sharing and amalgamation are being gazed at as the most ever more approved methodologies by governments around the globe, for solving problems in an extensive diversity of programs and policy areas. Protected information exchange is a noteworthy characteristic of every digital government that needs to give surety sovereign principles. Dares in building a computational infrastructure for exchanging privileged information is tricky to resolve and insist innovative motivation proposal. Finally, this paper presents well-organized enhanced PKI based information sharing security protocol for confidential sharing of secret information amongst security personnels and government intelligence sections in digital and mobile government environment. The wished-for trusted, cooperative and secure information sharing security protocol has offered privacy, validation, reliability and agency confirmation by utilizing MD5 Algorithm, public key infrastructure (PKI) and a unique and complex mapping function. In addition, on the basis of a predefined ranking of security personnel, a controlled privacy is preserved among the security personnel and government intelligence section. The usefulness of the wished-for security protocol has been established with the aid of experimental results.

Thus, digital government and mobile government demands more secure infrastructure, positive motivation, educational activity, trust and cooperation from government plus public. In conclusion, this article concludes that the secure wireless networks and better information sharing protocols are the key issues for implementing more successful digital government as well as mobile government worldwide.

Acknowledgements

I would like to thank Dr. G.K. Pradhan, Dr. Sanjay Biswas, Dr. Puthal, Dr. Mishra, Dr. B.B. Pradhan, Dr. A. Anjum, S. Anjum, Shabnam Mastari, Golam Ambia, Beauty, Abdul Wakil, Anuwarul Alam, Sohel, Tarannum and my father Md. Idrish plus mother Asma. I would like to thank also Dr. S. Dasgupta and Dr. Ganguli.

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 (2002): "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.
- [3] Robert D. Atkinson (2000): "Digital Government: The Next Step to Reengineering the Federal Government", *DC: Progressive Policy Institute*,
- [4] Jane E. Fountain (2004): "Preventing Chronic Disease, public health research, Practice, and Policy", Vol. 1: No. 4, October.
- [5] F.Arcieri, G.Melideo, E.Nardelli and M.Talamo (2002): "Experiences and issues in the realization of e-government services", *Proceedings of the 12th International Workshop on Research Issues in Data Engineering: Engineering e-Commerce/ e-Business Systems*, pp: 1066-1395.
- [6] James B. D. Joshi, Arif Ghafoor, Walid G. Aref and Eugene H. Spafford (2002): "Security and Privacy Challenges of a Digital Government", *Advances in Digital Government-Technology*.
- [7] Guido Bertucci (2007): "Managing Knowledge To Build Trust In Government", *United Nations Department of Economic and Social Affairs, United Nations Publication, New York*.
- [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 (2002): "Supporting Data and Services Access in Digital Government Environments".
- [10] 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.
- [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 (2008): "Secure information sharing for the U.S. Government", *White papers, Nortel Technical Journal*.
- [13] Peng Liu and Amit Chetal (2005): "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.
- [14] 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.

- [15] 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).
- [16] Xin L. (2007): "Distributed Secure Information Sharing Model for E-Government in China," *8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, Vol. 3, pp: 958-962.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] Tryg Ager, Christopher Johnson, Jerry Kiernan (2006): "Policy-Based Management and Sharing of Sensitive Information among Government Agencies," *MILCOM 2006*, pp: 1-9.
- [22] Thomas Casey, Alan Harbitter, Margaret Leary, and Ian Martin (2008): "Secure information sharing for the U.S. Government", *white paper, Nortel Technical Journal*.
- [23] Hui-Feng Shih and Chang-Tsun Li (2006): "Information Security Management in Digital Government", *Idea Group Publishing*, Vol. 3, pp. 1054 - 1057.
- [24] Peng Liu and Amit Chetal (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.
- [25] Rakesh Agrawal, Alexandre Evfimievski, Ramakrishnan Srikant (2003): "Information Sharing across Private Databases", *In SIGMOD '03: Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, pp. 86-97.
- [26] Ryan Layfield, Murat Kantarcioglu, Bhavani Thuraisingham (2008): "Incentive and Trust Issues in Assured Information Sharing", *International Conference on Collaborative Computing*.
- [27] Guido Bertucci (2007): "Managing Knowledge To Build Trust In Government", *United Nations Department of Economic and Social Affairs, United Nations Publication*, New York.
- [28] Theresa A. Pardo (2006): "Collaboration and Information Sharing: Two Critical Capabilities for Government", *Center for Technology in Government, University at Albany Annual Report*.
- [29] Md.Headayetullah, G.K. Pradhan (2009): "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.
- [30] Md.Headayetullah, G.K. Pradhan (2009): "Secure Information Sharing Between Government Intelligence Agencies: An Innovative Protocol Based on Trust", *International Journal of Engineering and Technology*, Vol: 1, No: 4, pp: 346-353.
- [31] Gail-Joon Ahn, Badrinath Mohan, Seng-Phil Hong (2007): "Towards secure information sharing using role-based delegation", *Journal of Network and Computer Applications*, Vol: 30, No: 1, pp: 42 - 59, January.
- [32] Mudhakar Srivatsa, Dakshi Agrawal, Steffen Reidt (2009): "A metadata calculus for secure information sharing", *Proceedings of the 16th ACM conference on Computer and communications security*, Chicago, Illinois, USA, pp: 488-499.
- [33] Muntaha Alawneh, Imad M. Abbadi (2008): "Preventing information leakage between collaborating organizations", *Proceedings of the 10th international conference on Electronic commerce*, Innsbruck, Austria, Article No.: 38.
- [34] Dunleavy, P. and Margetts, H, with John, S. and McCarthy, D. (1999) Government on the Web, London: *The Stationary Office, National Audit Office Report HC 87*, Session 1999-2000. See also: www.GovernmentOnTheWeb.org
- [35] Manish Kumar and Omesh Prasad Sinha (2008): "M-Government – Mobile Technology for e-Government", *Computer Society of India*.
- [36] Kushchu, I. and Kushchu, H (2003): "From E-Government to M-Government: Facing the Inevitable", *in the proceedings of European Conference on E-Government (ECEG 2003)*, Trinity College, Dublin.
- [37] Ghyasi, F. (2004): "Uses of Mobile Government in Developing Countries", web: <http://www.movlab.org>, accessed: 04.07.2004.
- [38] Md. Headayetullah et. al. (2010): "Proposed Conceptual Development Levels for Ideal Interoperability and Security in Modern Digital Government", *International Journal of Engineering Science and Technology*, Vol. 2(6), PP: 2218-2240.
- [39] Papazoglou, M. P., & Ribbers, P. M. A. (2006): "E-business: Organizational and technical foundations", *UK, West Sussex: John Wiley & Sons*.
- [40] Schooley, B. L., & Horan, T. A. (2007): "Towards end-to-end government performance management: Case study of interorganizational information integration in emergency medical services (EMS)", *Government Information Quarterly*, 24, PP: 755–784.
- [41] Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2007): "A collaborative network for first responders: Lessons from the CapWIN case", *Government Information Quarterly*, 24, PP: 785–807.
- [42] Luna-Reyes, L. F., Gil-Garcia, J. R., & Cruz, C. B. (2007): "Collaborative digital government in Mexico: Some lessons from federal web-based interorganizational information integration initiatives. *Government Information Quarterly*, 24, PP: 808–826.
- [43] Pardo, T. A., & Tayi, G. K. (2007): "Interorganizational information integration: A key enabler for digital government", *Government Information Quarterly*, 24, PP: 691–715.
- [44] Scholl, H. J., & Klischewski, R. (2007): "E-Government Integration and Interoperability: Framing the Research Agenda", *International Journal of Public Administration*, Vol.: 30(8), PP: 889–920.

- [45] King, W. R., & Teo, T. S. H. (1997): "Integration between business planning and information systems planning: Validating a stage hypothesis. *Decision Sciences*, Vol.:28(2), PP: 279–307.
- [46] Frankfort-Nachmias, C., & Nachmias, D. (2002): "Research methods in the social sciences, (5th Edition)", UK: Arnold.
- [47] Nolan, R. L. (1979): "Managing the crises in data processing", *Harvard Business Review*, PP: 115–126, March–April.
- [48] Earl, M. J. (2000): "Evolving the e-business", *Business Strategy Review*, Vol.: 11(2), PP: 33–38.
- [49] Rao, S. S., & Metts, G. (2003): "Electronic commerce development in small and medium sized enterprises: A stage model and its implications", *Business Process Management*, Vol.: 9(1), PP: 11–32.
- [50] Gottschalk, P., & Tolloczko, P. C. (2007): "Maturity model for mapping crime in law enforcement", *Electronic Government, an International Journal*, Vol.: 4 (1), PP: 59–67.
- [51] Kazanjian, R. K., & Drazin, R. (1989): "An empirical test of a stage of growth progression model", *Management Science*, Vol.: 35(12), PP: 1489–1503.
- [52] Chen, Z., Gangopadhyay, A., Holden, S. H., Karabatis, G., & McGuire, P. (2007): "Semantic integration of government data for water quality management", *Government Information Quarterly*, Vol.: 24, PP: 716–735.
- [53] Tryg Ager, Christopher Johnson, Jerry Kiernan (2006): "Policy-Based Management and Sharing of Sensitive Information among Government Agencies," *MILCOM 2006*, pp: 1-9.
- [54] Arazyan H. (2002): "m-Government: Definition and Perspectives", web: http://www.developmentgateway.org/download/143909/mGov_Interview_2.doc, accessed: 17.07.2004
- [55] Lallana, E (2004): "E-Government for Development, M-Government Definitions and Models", web: <http://www.egov4dev.org/mgovdefn.htm>, accessed: 12.04.2004
- [56] Antovski, Lj. & Gusev M., (2003): "New Mobile Payments Model", *Proc. of the SSGR*, Roma, Italy.
- [57] Sadeh, Norman (2002): "M-Commerce: Technologies, Services and Business Models", *John Wiley and Sons, Inc*, Canada and USA
- [58] Md. Headayetullah and G. K Pradhan (2010): "Efficient and Secure Information Sharing For Security Personnels: A Role and Cooperation Based Approach", *International Journal on Computer Science and Engineering*, Vol. 02, No. 04, pp: 1254-1265.
- [59] Md.Headayetullah, G.K. Pradhan, Sanjay Biswas, B. Puthal (2011): "Proposed Information Sharing Security Approach for Security Personnels, Vertical Integration, Semantic Interoperability Architecture and Framework for Digital Government", *International Journal of Computer Science & Information Technology (IJCSIT)*, Vol. 3, No. 3, PP: 120-139.

Authors:

Dr. 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 received Ph.D in Computer Science & Engineering degree with First Class with Honours from the Department of Computer Science and Engineering from Institute of Technical Education & Research (Faculty of Engineering) of Siksha O'Anusandhan University (SOAU), Bhubaneswar, India in 2010-2011 (23rd July). He is currently gathering some Post Doctoral or Post PhD experience, working closely with Prof. (Dr.) G.K Pradhan and Prof. (Dr.) Sanjay Biswas in the Department of Computer Science and Engineering (Faculty of Engineering) of Siksha O'Anusandhan University (SOAU), Bhubaneswar, India. His fields of interest are Mobile Government, E-Government, Digital Government, E- Commerce, Networking, Internet Technology, Data Privacy, Cryptography, Information Security and Mobile Computing. He has authored more than 7 Research Publication in International Journal. He is currently working as an Associate Professor in the PG department of Computer Science & Engineering and Information Technology at Bengal College of Engineering & Technology, Durgapur, West Bengal University of Technology, Kolkata, India. He has more than 8 years teaching experience in the department of Computer Science & Engineering. He serves as an editorial member and reviewer in many International Journals worldwide. Dr. Headayetullah serves as an authorized research supervisor for PhD degree in the field of Computer Science and Engineering and IT in many Universities in India. He is writing books for Mobile Computing and Computer Organization & Architecture and Digital Government subjects for UG and PG level student in the field of Computer Science & Engineering. Prof. (Dr.) Headayetullah is the members of IAENG and IACSIT respectively.

Dr. 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.

Dr. A. Anjum has keen interest on Computer Science & Engineering and Information Technology. Her research areas are Genetic Algorithm, Biotechnology and Medical Sciences. She provides free medical services to the wide-ranging poor people in our society.