Name of Research Scholar:	**Muzaffar Azim**
Name of Supervisor:	**Prof. M.N. Doja, Hony. Director, FTK-CIT**
Department/ Center:	**FTK- Center for Information Technology**
Title of Thesis:	**A Framework for Securing e-Governance**

ABSTRACT

Now-a-days the whole paradigm of governance has changed. The emergence of Information & Communication Technology (ICT) and new computing paradigms have provided significant opportunities to the Governments for faster & better information processing leading to speedier and qualitative better decision making, greater accountability, wider reach, better utilization of resources; thus overall good governance. A technology that has the potential to offer solutions for e-governance is Cloud computing. Cloud computing is a new way of providing services over internet. Cloud based e-Governance system provides services at reduced cost and manages security, scalability & accountability well. Although there are many advantages of Cloud computing, issues related with security & privacy are some of the major challenges, which need to be addressed for the successful deployment of a Cloud based e-Government System. The security of e-Government is a crucial issue and a basic level of confidence & security must be established so that the e-citizens are able to trust and use e-services.

Governments around the world are using Cloud computing in a big way. Moving e-Governance to the Cloud changes the risks associated with the Government organization. Cloud Security Alliance (CSA) says that insufficient due diligence is among the top threats in Cloud computing. This threat is linked to the fact that organizations which strive to adopt Cloud computing often do not understand well the resulting risks. Therefore it is absolutely critical for any Government organization to identify and quantify the risks associated with the implementation of the Cloud. Further, organizations should have a proper risk management system to manage and mitigate these risks.

During literature survey, it has been found that there are some security risk assessment & management standards released by governments and private organizations such as NIST, CSA, ENISA and ISO, which have released standards. Although these standards are generic standards but are not specific for the Cloud environment. Some research work has also been done in proposing risk assessment & management model in the Cloud, but these works are limited to specific security problems.

In view of the lack of security standards and security assessment and management approaches available in Cloud environment as mentioned above, the goal of this research work was to propose a Security Framework for Government Organizations in Cloud environment. To achieve this goal, the research work has first of all introduced a new set of Security Control Principles/Security standards called e-Government Security Matrix (eGSM) especially for the Cloud based e-Governance Systems. The eGSM consists of four Security Domains and twenty key risk factors called Security Control Areas. The eGSM can serve as a security assessment index system for the e-Governance. It can provide a suitable reference to the Cloud Service Providers, Third Party Assessment, Audit and operation of the System as well as for other business requirements.

Further the research work has proposed an e-Governance Security Assessment Model (eGSAM) to assess the security level of the whole system as well as security levels of each Security Domain. The model also determines the relative importance weight & ranking at each security Domain; as well as the risk value weights & ranking of the twenty risk factors. As a result, the users of the system are in a position to prioritize the process for the high value risks. The model is based on Analytical Hierarchy Process and Fuzzy Comprehensive Evaluation Method which combines Fuzzy Mathematics with Expert's expertise to determine security level of the System at each level.

The research work has also proposed a new e-Governance Security Framework (eGSF) for a Cloud based e-Governance Systems. The most important feature of the proposed Security Framework is to devise a mechanism through which an organization can have a path of improvement along with understanding of the current security maturity level & defining desired state in terms of security metric value.