A SECURITY FRAMEWORK FOR CLOUD BASED E-GOVERNANCE SYSTEM

Muzaffar Azim¹, Dr. S. Kazim Naqvi²
¹,² FTK Centre for Information Technology, Jamia Millia Islamia, New Delhi, (India)

ABSTRACT
The exponential growth of Cloud computing is changing the way organizations are functioning now a days. A Cloud based system changes the services seamlessly without expending much time and resources in setting up new systems. Apart from this, there are lots of benefits like scalability, significant cost reduction, high availability and quality in a Cloud based System. Although there are many advantages of Cloud computing, issues related with Security & Privacy are some of the major challenges, which needs to be addressed for the successful deployment of a Cloud based System. Therefore, it is absolutely critical to have a robust Security services fully implemented based on Security Framework/Guidelines. At present there are a number of standard Security Framework/Guidelines like ISO 27001/27002, NIST 800-53, but all these standards are in evolving stage for the Cloud Computing Environment. Apart from this, the security requirements of an organization also vary based on specific Security risks of the Organization. This paper first introduces a new set of Security Control Principles called e-Government Security Matrix (EGSM) specially for the Cloud based e-Governance Systems and then proposes a new e Governance Security Framework (EGSF).

Keywords: E-Governance, Security Framework, Security Requirements, Cloud Computing.

I. INTRODUCTION
The exponential growth of Internet has not only changed our life, but it has also changed the functioning and service delivery models of the governments. The rise of e-Government has been one of the most important developments of the web. E-Governance is the application of Information and Communication Technologies (ICT) to exchange information between the government and the citizens, government and businesses and between government organizations [1]. According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2]. 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 [3]. The available resources such as storage, memory, processing power and bandwidth are used efficiently in a Cloud based system. It also ensures high availability and quality. Although there are many advantages of Cloud Computing, issues related with Security & Privacy are some of the major challenges, which needs to be addressed for the successful deployment of a Cloud based e-Government System [4]. Security of information means confidentiality, integrity, proper authentication and reliability of Information. The issue of Security and Privacy is further enhanced in a cloud based e-Governance System as the confidential data is being stored outside the physical
boundary of the Organisation. Therefore, it is absolutely critical to have a robust Security services fully implemented based on Security Framework/Guidelines. At present there are a number of standard Security Framework/guidelines like ISO 27001 [5]/27002 [6], NIST 800-53 [7], but all these standards are in evolving stage for the Cloud computing environment. Although ISO/IEC 27001 provides generic guidance in developing the security objectives and metrics, but it still does not provide methods to guide the organizations [8]. Apart from this, the security requirements of an organisation vary based on the specific security risks of the Organisation. Therefore it is absolutely essential to have a comprehensive end-to-end Security Framework based on industry Standards, but tailored to the specific requirement of an Organisation. During literature survey it has been found that very limited work has been done in the field of Security Framework of an e-Governance system especially for a Cloud based e-Governance system. While reviewing Industry Security Framework and Guidelines, it was found out that there are no Cloud Security Frameworks, best practices and Guidelines for a Cloud based e-Governance System. This paper first introduces a new set of Security Control Principles called e-Government Security Matrix (EGSM) specially for the Cloud based e-Governance Systems based on the Security Control Principles described by Vic (J.R.) Winkler [9] and after mapping the security requirements of other industry standard Frameworks like ISO 2001, Cloud Control Matrix (CCM), NIST SP 800-144. A new e-Governance Security Framework (EGSF) has also been proposed for such Cloud based e-Governance Systems. The most important feature of the proposed Security framework is to devise a mechanism through which an organisation can have a path of improvement along with understanding of the current security maturity level & defining desired state in terms of security metric value. The Paper is organised as follows: Section 2 presents the existing work on Cloud Security and Security Maturity Levels. Section 3 presents the new set of Security Control Principles called e-Government Security Matrix (EGSM). Section 4 presents the Proposed Security Framework for Cloud Based e-Governance (EGSF). Section 5 presents Conclusion and future work.

II. EXISTING WORK ON CLOUD SECURITY GUIDANCE OR FRAMEWORKS

There are several Organisations/consortia actively involved in the development of security standards/ guidelines. Some of the Cloud Security Framework/Guidelines being developed by several consortia/organizations are as following:

2.1 National Institute of Standards and Technology

(NIST) has released special drafts and reports on security issues as well as recommendations for the Cloud computing. It has released a special publication “Guidelines on Security and Privacy in Public Cloud Computing (NIST SP 800-144)” [10]. The Guidelines provide, in NIST’s description: "an overview of the security and privacy challenges facing public cloud computing and presents recommendations that organizations should consider when outsourcing data, applications and infrastructure to a public cloud environment. The document provides insights on threats, technology risks and safeguards related to public cloud environments to help organizations make informed decisions about this use of this technology.” The recommendations have been given in following Areas:

1. Availability
2. Identity and Access Management
3. Architecture
4. Software Isolation
5. Data Protection  
6. Incident Response  
7. Compliance  
8. Trust  


The ISO/IEC 27000 family of information security standards is developed and published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). It is one of the most widely used Security Framework for the information security and management. The security standards related with the Cloud Computing are as following:  

2.2.1 ISO/IEC 27002:2013 [11] is the Security Framework which describes the security control objectives and controls. The twelve guiding security control principles of the ISO/IEC 27002 are:  

1. Access control  
2. Physical and environmental security  
3. Risk assessment and treatment  
4. Security policy  
5. Organisation of information security  
6. Assets management  
7. Communications and operations  
8. Information systems acquisitions, development and maintenance  
9. Information security incident management  
10. Business continuity management  
11. Human resource security  
12. Compliance  

2.2.2 ISO/IEC 27017  
The ISO/IEC 27017 [12] is in draft stage and will provide a Framework for some additional security controls beyond provided in ISO/IEC 27002. This standard will provide guidance on the information security elements of Cloud computing, recommending and assisting with the implementation of Cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards [12].  

2.2.3 ISO/IEC 27018  
The ISO/IEC 27018 is a Security Framework which covers PII (Personally Identifiable Information) in public clouds.  

2.2.4 ISO/IEC 27036:2013+  
The ISO/IEC 27036:2013+ is a multi-part Security Framework for providing guidelines for supplier relationships including the relationship management aspects of cloud computing (parts 1, 2 and 3 have been published so far) [13].
2.2.5 ISO/IEC 21827: Systems Security Engineering Capability Maturity Model

The Systems security engineering capability maturity model (SSE-CMM) is also known as the ISO/IEC 21827 standard [14]. It defines five levels of maturity models as shown in Fig.1 below:

![Maturity ladder diagram]

**Figure 1: System Maturity Model**

2.3 Cloud Security Alliance (CSA)

The CSA alliance provides advice for both Cloud computing customers as well as for Cloud Service Providers. The Cloud Security Alliance Cloud Controls Matrix (CCM) [15] is the Security Framework for guiding cloud vendors and prospective cloud customers in assessing the overall security risk of a Cloud provider. The Framework is based on other industry-accepted security standards, regulations, and controls Frameworks such as the ISO 27001/27002, NIST, ISACA COBIT, PCI and Jericho Forum [15]. The CSA CCM Framework provides information regarding information security control requirements. It identifies security threats and vulnerabilities in the Cloud as well as provides information regarding standardized security and necessary security measures to be taken. Various strategic domains as covered in CCA CCM (CSAguide version 3.0) are as follows:

1. Application & Interface Security
2. Audit Assurance & Compliance
3. Business Continuity Management & Operational Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Data Centre Security
7. Encryption & Key Management
8. Governance and Risk Management
9. Human Resources
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Threat and Vulnerability Management
16. Supply Chain Management, Transparency and Accountability
2.4 Distributed Management Task Force (DMTF)
The Distributed Management Task Force (DMTF) is an organization which is actively involved in the development, adoption and interoperability of management standards and initiatives for the enterprise and Internet environments [16]. It has established a Framework to promote standards for Cloud security and interoperability between Clouds.

2.5 Storage Networking Industry Association (SNIA)
The Storage Networking Industry Association (SNIA) [17] has developed an Framework, Cloud Data Management Interface (CDMI), which is an open standard for data storage as a service as part of Cloud computing.

2.6 Open Grid Forum (OGF)
The Open Cloud Computing Interface (OCCI) [18] is a Framework developed by Open Grid Forum. OCCI is a Protocol and API for all kinds of Management tasks, which was originally developed for creating remote management API for IaaS model based Services. The current release of the Framework is now suitable to all models (IaaS, PaaS and SaaS) and addresses all technical and operational security issues in the grid and Cloud environments.

2.7 Association for Retail Technology Standards (ARTS)
The Association for Retail Technology Standards (ARTS) Version 2.0 is a Framework for the Cloud Computing in Retail. The Framework provides guidelines for the reliability, availability and security for Cloud-based solutions. [19]

2.8 Cloud Standards Customer Council (CSCC)
Cloud Standards Customer Council (CSCC) [20] is an end user advisory group working for the acceleration of Cloud adoption and addressing security and interoperability issues surrounding the transition to the Cloud. The council provides Cloud users with the opportunity to drive client requirements into standards development organizations and deliver materials such as best practices and use cases to assist other enterprises [20].

2.9 Organization for the Advancement of Structured Information Standards (OASIS)
OASIS (Organization for the Advancement of Structured Information Standards) is an international consortium for promoting the adoption of product-independent standards for information formats such as Extensible Markup Language (XML), Standard Generalized Markup Language (SGML), and Hypertext Markup Language (HTML)[21]. The OASIS Cloud Application Management for Platforms (CAMP) Technical committee has developed an interoperable protocol that Cloud implementers can use to package and deploy their applications. It defines interfaces for self-service provisioning, monitoring, and control [22].

III. PROPOSED CLOUD BASED E-GOVERNANCE SECURITY MATRIX (EGSM)
Several Cloud Security Framework and Guidelines have been described in last section. While reviewing those Security Framework and guidelines, it was found out that there is no Cloud Security Framework, best practices, and guidelines defined as per the specific security requirements of a Cloud based e-Governance System. The new set of Security Control Principles called e-Government Security Matrix (EGSM) is based on the security
Control Principles described by Vic (J.R.) Winkler [9] as well as other industry standard Frameworks like ISO 2001, Cloud Control Matrix (CCM), NIST SP 800-144. It consists of four Security Control domains as following:

1. Foundational Security Domain
2. Deep Defence Domain
3. Operational Security Domain
4. Business requirement Domain

Each domain is further divided into different Security Control Areas as shown in the fig. 2 below:

![Fig.2: e-Government Security Matrix (EGSM)](image)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FS1</td>
<td>Security Policy</td>
<td>Security Policy</td>
<td>FS1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Principles &amp; Standards</td>
<td>FS1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Guidelines &amp; Procedures</td>
<td>FS1.3</td>
</tr>
<tr>
<td>FS2</td>
<td>Cloud Service Providers (CSP)</td>
<td>Cloud Service Providers (CSP) Management</td>
<td>FS2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Requirements of CSPs</td>
<td>FS2.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security in CSPs Operations &amp; Support System</td>
<td>FS2.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSP Audit &amp; Compliance</td>
<td>FS2.4</td>
</tr>
<tr>
<td>FS3</td>
<td>Third Party Providers (TPA)</td>
<td>Third Party Providers (TPA) Management</td>
<td>FS3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Requirements of TPAs</td>
<td>FS3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security in TPAs Operations &amp; Support System</td>
<td>FS3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPA Audit &amp; Compliance</td>
<td>FS3.4</td>
</tr>
<tr>
<td>FS4</td>
<td>Personnel Security</td>
<td>Security prior to employment</td>
<td>FS4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security during Employment</td>
<td>FS4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security after change of Employment</td>
<td>FS4.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Awareness &amp; Training</td>
<td>FS4.4</td>
</tr>
</tbody>
</table>

Table 1: Security Control Domain 1 (Foundational Security)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DD1</td>
<td>Identity &amp; Access Management</td>
<td>Federated Identity Management</td>
<td>DD1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privileged Identity Management</td>
<td>DD1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Access Requirements</td>
<td>DD1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Access Management</td>
<td>DD1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application &amp; Information Access Management</td>
<td>DD1.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hypervisor &amp; O/S Access Control</td>
<td>DD1.6</td>
</tr>
<tr>
<td>DD2</td>
<td>Security of Service Delivery Model</td>
<td>Service Delivery Models (Saas Paas, Iaas) Management</td>
<td>DD2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security in Service Delivery Model Operations</td>
<td>DD2.2</td>
</tr>
<tr>
<td>DD3</td>
<td>Host &amp; VM Security</td>
<td>Security Requirements of Host &amp; VM</td>
<td>DD3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security of Host &amp; VM</td>
<td>DD3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtualization</td>
<td>DD3.3</td>
</tr>
<tr>
<td>DD4</td>
<td>Appln. SW Quality Assurance</td>
<td>Application &amp; Software Maintenance</td>
<td>DD4.1</td>
</tr>
<tr>
<td>DD5</td>
<td>Network Security</td>
<td>Network Security Management</td>
<td>DD5.1</td>
</tr>
<tr>
<td>DD7</td>
<td>Cryptography &amp; Key Managmt.</td>
<td>Cryptographic Control &amp; Key Management</td>
<td>DD7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Access Management</td>
<td>DD7.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application &amp; Information Access Management</td>
<td>DD7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hypervisor &amp; O/S Access Control</td>
<td>DD7.4</td>
</tr>
</tbody>
</table>

Table 2: Security Domain 2 (Deep Defence)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OS1</td>
<td>Physical &amp; Environment Security</td>
<td>Physical Access Management</td>
<td>OS1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Environmental Control</td>
<td>OS1.2</td>
</tr>
<tr>
<td>OS2</td>
<td>Assets Management</td>
<td>Assets Control Management</td>
<td>OS2.1</td>
</tr>
<tr>
<td>OS3</td>
<td>Governance and Risk Mangmt.</td>
<td>Risk Management</td>
<td>OS3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat and Vulnerability Management</td>
<td>OS3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Governance</td>
<td>OS3.3</td>
</tr>
<tr>
<td>OS4</td>
<td>Security Incident Management</td>
<td>Security Incident Management</td>
<td>OS4.1</td>
</tr>
<tr>
<td>OS5</td>
<td>Operation Practices</td>
<td>Operation Control</td>
<td>OS5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration Management</td>
<td>OS5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Media &amp; Memory Protection</td>
<td>OS5.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fail-safe Protection</td>
<td>OS5.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Denial of Service Protection</td>
<td>OS5.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Partitioning</td>
<td>OS5.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Function Isolation</td>
<td>OS5.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Honeypots</td>
<td>OS5.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Boundary &amp; Session Protection</td>
<td>OS5.9</td>
</tr>
</tbody>
</table>

Table 3: Security Domain 3 (Operational Security)
Table 4: Security Domain 4 (Business Requirements)

IV. E-GOVERNMENT SECURITY FRAMEWORK (EGSF)

The proposed e-Government Security Framework (EGSF) is composed of the following building blocks as given in Fig.3:
Step-1: **Selection of Control Areas**: The selection of Security Control Areas (group of Security Control Principles) is the first step for the development of a comprehensive Security Framework. The Paper has presented a new set of Security Control Areas/Principles called e-Government Security Matrix (EGSM) applicable for a cloud based e-Government System in last section. However, the security requirements of an organisation change continuously in view of emerging new threats and vulnerabilities, therefore it is absolutely necessary to map the security control Areas of the EGSM with other Security Framework/guidelines like ISO 27001/27002, NIST 800-53 and fill the gap, if any.

Step-2: **Identify & Define Control Principles**: Once different Security Control Areas (group of Security Control Principles) have been identified as discussed in last step, it needs to be broken down into different Security Control Principles. The Security Control principles should be practical and should be customised based on business requirements of the Organisation.

Step-3: **Build Requirement Cross Matrix**: Most industry Security Standards, while different, are based on the same security principles/requirements, therefore, similarities among the standards should be grouped together and combined.

Step-4: **Develop & Prioritize Requirements**: Once security requirements have been finalized based on mapping of different Security standards and guidelines, it is very important to prioritize the requirement based on constraints of available resources as well as after identifying both the impact and risk exposure. A cost analysis of the resources required for carrying out requirement is very useful in prioritizing the requirements.

Step 5: **Security Policy Formalization**: The next step of the Security Framework is to create and define a clear policy based on the security requirements finalized in last step. Policies set organizational direction and carry the weight of management. Policies should be updated as per need. Security policy states the reasons and identifies the rules, standards. It says what must be done whereas the guidelines say how it should be done.

Step-6: **Develop Security Measurement & Metrics**: An effective Security Measurement System is very critical to assess the effectiveness of the implemented technical security controls and to ensure safeguard against current and future attacks. The mandatory requirement in ISO/IEC 27001 standard clause 4.2.2(d) says that “Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results”. The development of technical security metrics should be more focused on the critical security controls that provide high impact to the organisation. Metrics should be SMART: Specific, Measurable, Attainable, Relevant & Timely. There are internationally accepted Frameworks available for the Metrics Developments like Common Assurance Maturity Model (CAMM), IT Infrastructure Library (ITIL), Control Objectives for Information and related Technology (CobiT), ISO/IEC 27002 / ISO 27004 [2] / NIST 800-55 [3]. Metrics can be composed of sub-metrics as well as Group Metrics could also be formed combining different Metrics.

Step-7: **Establish Security & Metric benchmarks and targets**: The next step of the Security Framework is to establish security & Metrics benchmarks and Targets, which is very important step of the Framework. Appropriate benchmarks would be set up for all the five maturity levels of Security Framework for each Metric & Group Metric. Benchmarking will be done comparing the performance & practices of the Organisation.
against the peers within the industry. It will ensure that Targets set are achievable as well as for ensuring improvements in the existing practices, which is critical for the success of the Framework. The national and global metrics provided by various professional associations and published research are also very helpful. Apart from this the each Metric/sub Metric could be assigned a corresponding weight based on the Common Vulnerability Scoring System (CVSS) Score. The CVSS base score is calculated using the information provided by the U.S. National Vulnerability Database (NVD) Common Vulnerability Scoring System Support v2 [20]. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

**Step-8: Security & Metric Evaluation:** The Security & metric evolution is a very important step in Security Framework. It is a measurement for all the Users, virtual machine and Security Services implemented. Automatic metric Collection is the ideal situation, however wherever automatic metric collection is not possible, it will be done manually through System logs, questionnaires, interviews of the understanding, perceptions and implementation of Experts. Security metrics can be calculated in the form of a weighted sum [24]. It will be calculated at Metric Level & Group Metric level.

\[ M_1 = w_{M1.1} \cdot \overline{M_{1.1}} - w_{M1.2} \cdot \overline{M_{1.2}} - w_{M1.3} \cdot \overline{M_{1.3}} \]

Where \(M_1\) is value of Metric 1; \(w_{M1.i}\) denotes weight of Sub metric/components \(M_{1.i}\)

\(\overline{M_{1.i}}\) denotes normalized and uniform scaling of the components metrics

The measured Metric value will be compared with the benchmark set to know the maturity level for each Metric and Group metric. These values will be analysed and necessary steps will be taken to further improve the security of the System. Thus the most important feature of the proposed Security Framework is to devise a mechanism through which an organisation can have a path of improvement along with understanding the current security maturity level & defining desired state in terms of security metric value/maturity level.

**V. CONCLUSION & FUTURE WORK**

The rapid emergence of Cloud computing is transforming the way organizations are functioning now a days. Although there are many advantages of Cloud Computing, issues related with Security & Privacy are some of the major challenges and obstacles, which need to be addressed for the successful deployment and operation of e-government. While reviewing Industry Security Framework and guidelines, it was found out that there are no Cloud Security Framework, best practices, and guidelines that meet the complete needs of an cloud based e-Governance System. This paper first introduces a new set of Security Control Principles called e-Government Security Matrix (EGSM) especially for the Cloud based e-Governance Systems. A new e Governance Security Framework (EGSF) has also been proposed for such Cloud based e-Governance Systems. The validation of this proposed Security Control Matrix by industry Experts through questionnaires can be taken as a future work. The mapping of different Security Control Principle described in this Paper with other important industry Standards like ISO 2002/20017, Cloud Security Alliance Cloud Controls Matrix (CCM) can also be taken as future work. The Proposed security Control Matrix has defined the Security Control Areas for Cloud Based e-Governance System, identifying/defining some useful Matrices can be taken as important future work.
REFERENCES


[10] NIST SP 800-144, csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf


