Security Engineering in G-Cloud: A Trend towards Secure e-Governance

Priyank Singh Hada
Central University of Rajasthan, Kishangarh

Ranjita Singh
Central University of Rajasthan, Kishangarh

Deepshikha Goyal
Central University of Rajasthan, Kishangarh

ABSTRACT
Government is nowadays trying to improve efficiency using technologies from IT industry to stimulate its processes more efficiently and faster. Hence, e-Governance was brought into existence, e-governance provided services like e-banking, fund transfer, e-billing, online registration etc online. To ameliorate things further and introduce more advantages, it was proposed to rebuild e-Governance applications and services in terms of cloud computing which we call Government-Cloud (G-Cloud). G-Cloud gathers its set of benefits of centralization, scalability etc. from cloud computing and also caters security benefits to e-Governance. But with this comes many security risks which have to be brought under consideration. In this paper we are discussing the security benefits of G-Cloud and also risks associated with this reconstruct.

General Terms
Security Management, e-Governance, Cryptography, Cloud security.

Keywords
e-Governance, Cloud computing, G-cloud, Security issues, Security benefits.

1. INTRODUCTION
In Indian scenario to cope with government system is an inevitable task in every person's routine, whether it's a ration card application, passport service, information sharing, bill payment, tax filling, banking, social services etc. But these services are accessible in a very slow and time consuming manner. The reason behind this is the fact that whole system is manual. So there is a canonical need of bringing in transparency, efficiency and reliability in the governance system. For this information technology was introduced with government services and called e-governance which made all these services easily accessible for common man [1]. Looking at the unpredictable resource requirements, implementation efforts and high expenditure, it was proposed to rebuild e-governance services in terms of cloud computing. Cloud computing provides an on demand scalable pool of resources which can be accessed ubiquitously over internet. This reconstruct of e-governance services is termed as *Government-Cloud* (G-Cloud). As G-Cloud includes cloud computing so it is always talked about in terms of its convenient infrastructure and service supply but its security issues are put to lower priority. Moreover, G-Cloud is conceived for e-Governance so it is required that security must be put to forefront of consideration. Therefore, this paper is divided into seven sections. Second and fourth section contribute introduction to e-Governance and its security requirements. Then third and fifth section introduces cloud computing and its benefits to e-Governance system.

2. E-GOVERNANCE
Stated simply, "e-Governance" or Electronic Governance is defined as acquisition of government services and information ubiquitously by the citizens and other organizations through Information and Communication Technologies (ICTs) from government agencies to support good governance for the following reasons [2]:

- Information sharing between organizations, citizens and government departments
- Faster delivery of public services
- Efficiency and reliability
- Cost effectiveness and revenue benefits
- Transparency

e-Governance is not only about facilitating e-mail, internet and service delivery but will also change the way individuals interact with government to access citizen centric services.

2.1 Why e-Governance?
For the government to work efficiently and reliably, it has to work in harmony with business organizations, citizens and government bodies. This makes the information flow between government and citizen more meaningful and speedy. The advantages of bringing in this system which would also save time and money for all concerned are:

- Provide faster, effective and timely government services.
- Effective integration of government into the community itself.
- Concentration of resources where they are highly needed.

Developing nations face a lot of challenges and responsibilities to bring themselves in level with developed nations which can only be circumvent by bringing in e-governance reforms. e-Governance does this task by improving government processes, connecting citizens and bringing in interactions within the public forums. e-Governance interactions include communication from government to business, citizens, enterprises, NGOs and other government departments. Figure1 describes these interactions in terms of services provided to these bodies by e-governance.

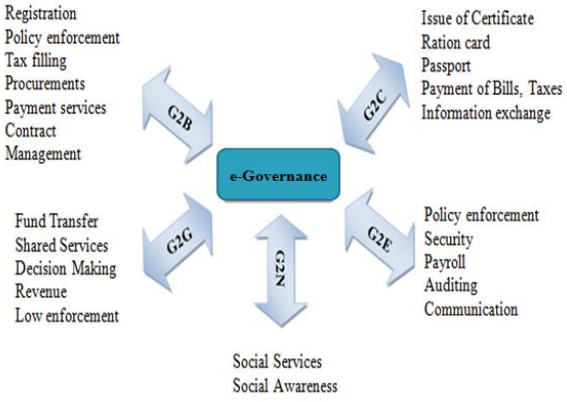

Figure 1: e-Governance service delivery models and applications

2.2 Scope of E-Governance

e-Governance has the following dimensions to support good governance [3]:

3.2.1 Government to Citizen (G2C)

Citizens can access various e-Governance services like issue of Certificates, Ration Cards, Passports, Payment of Bills, taxes and information about health, employment, agriculture and social services etc.

3.2.2 Government to Government (G2G)

Government bodies can share information and interact with each-other for the applications like fund transfer, shared services, decision making, revenue and low enforcement etc. All of these applications require a high degree of message passing across department.

3.2.3 Government to Business (G2B)

Business organizations provide or use information to government in terms of registration, policy enforcement, tax filling, procurements, payment services and contract management etc. The biggest area for interaction is contract management.

3.2.4 Government to Enterprise (G2E)

Government controls the various Enterprises like Water Board, Electricity for policy enforcements, security, payroll, auditing (for accountability) and communication etc.

3.2.5 Government to NGO (G2N)

Government also involves in building of various associations or interested groups that ensure the betterment of the society. Such initiatives deal with the relationship between government and citizens from whom the public sector derives its legitimacy, or as customers who consume public services.

e-Governance services require on demand scalable resources which can be accessed over a broad network. For example, in passport system, it is unpredictable how much storage will be required in future and also to avail the services ubiquitously, broad network access is a necessary requirement. Also server usage for passport service is not so high that we provide a dedicated server for this purpose. Unnecessary usage must be avoided so that only payment is done on pay per use basis. All these requirements can only be satisfied with cloud computing characteristics. So this brings in cloud computing framework to fulfill e-governance service requirements.

3. CLOUD COMPUTING

Cloud computing is the delivery of dynamically scalable IT resources over the internet instead of hosting them locally or local LAN to meet the changing business needs. The resources can be any services, computing, storage or even infrastructure.

As these resources are available over the network, any organization or user can buy them on as needed basis and avoid costs of software and hardware. Cloud does not allocate resources for static set of applications, instead a set of resources are allocated ad hoc to run applications. In a cloud computing environment, a user (via a virtual desktop, for example) requests information from an application. The cloud computing environment must then broker resources to run that application. The address of the allocated resources is returned and applications execution proceeds. Virtualization is the key element in any form of application or resource brokering.

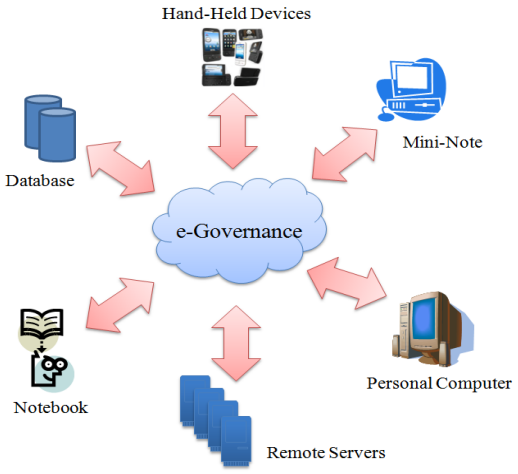

Figure 2: Cloud Architecture

Clearly this definition summarizes services, deployment models and characteristics of cloud.

3.1 Cloud Characteristics [4]

Cloud computing environment has following characteristics:

1. On Demand Service: User can avail the resources instantly without having to physically interact with the service provider.
2. Broad Network Access: Services accessed via internet using standard protocols and methods.
3. Resource Pooling: A homogeneous infrastructure is used for realization of cloud services by the service providers.
4. Rapid Elasticity: Resources can be scaled up or down as per need.
5. Measured Service: Resource usage is continuously monitored for billing purpose as services are provided on pay per use basis.

3.2 Service Models of Cloud Computing

Cloud services come in many flavors depending on the type of resources provided by cloud [4]:

3.2.1 Software as a Service (SaaS)

In this service, applications and computational resources required to run them are provided to the user on demand. Total cost of hardware and software deployment and

maintenance is reduced. Underlying infrastructure is controlled and managed by cloud provider. User has to set only preferences and administrative application settings. Example, Google Mail, Google Docs, etc.

3.2.2 Data/Storage as a Service (DaaS or SaaS)

Data is stored at service provider site and customer can query that data on demand regardless of the geographic location of data. It allows for the separation of data cost and usage from specific software or platform. As an example, Amazon S3, Google BigTable provides data storage services.

3.2.3 Platform as a Service (PaaS)

In this cloud computing environment platform is provided as on demand service over which user can deploy and develop desired applications. The deployment environment can be rented on demand and are special purpose designed on the basis of customer needs. As an example, Google AppEngine provides platform as a service.

3.2.4 Infrastructure as a Service (IaaS)

A basic computing infrastructure like servers, software, and network equipment is provided as an on-demand service upon which a platform can be deployed and applications can be executed. Infrastructure components for a system need not to be bought, instead can be obtained as virtualized objects controlled via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. As an example, Amazon's EC2, GoGrid provides such services.

3.2.5 Identity and Policy Management as a Service (IPMaaS)

IPMaaS service provider manages the identity and policy issues of customer. Customer relies on service provider to perform some function on data provided by user so that his identity can be authenticated. Also an enterprise or individual asks service provider to check whether certain functionality or new technology introduced in system obeys the policies of the enterprise.

3.2.6 Network as a Service (NaaS)

Here virtual networks are provided to the users which are made available by service provider. Virtual Private Network (VPN) is an example of cloud service in which cloud can serve as a network system which is secure as well as maintains privacy of the user.

3.2.7 Hardware as a Service (HaaS)

In this model cloud can offer services requiring particular hardware, results of which can be used by the user, so that user doesn't have to buy the hardware resources.

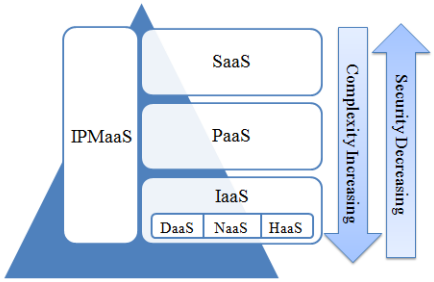

Figure 3: Cloud Service Models

3.3 Cloud Deployment Models

With above described levels of services cloud provides following deployment models to define the scope of cloud services [4].

3.3.1 Public cloud

Resources are available to multiple users who can quickly access them as per-use basis via web services. Resources are provided by a single service provider who can bill the usage. It suffers from security and compliance disadvantages.

3.3.2 Private cloud

Instead of keeping your private data to a third party service provider private cloud keeps it to the private enterprise only. Internal personnel manage and control the cloud data and are visible to enterprise only. Its advantage is that it solves security and compliance problems.

3.3.3 Community cloud

A group of organizations or enterprises jointly creates a cloud infrastructure which share resources between over a common cloud. This cloud can be hosted by a third party or by one of the organization in the group.

3.3.4 Hybrid cloud

It is combination of public and private cloud. It follows private cloud rules during normal workload of enterprise but shifts to private cloud and uses its resources when workload goes to peak and gets back to using private resources when workload resumes to normal being.

3.3.5 G-Cloud

'G-Cloud' initiative by UK Government is a futuristic vision for Government Cloud Computing. G-Cloud offers the cloud as base platform for government application services and interactions, reducing cost through data-center consolidation, improving operations through virtualization, but the main benefit will come from how it changes ICT procurement model and the compounding effect this has in improving how all of government itself works. This initiative has most remarkable aspect of how it will change the interaction among government bodies and society. G-Cloud enables open government cloud computing, thus making government more transparent in terms of its accountability to public. This also makes government more available for public services, decision making and communication purposes. G-Cloud makes government open in terms of technology and data [11]. Public can access any information under Right to Information act for which they would not have to undergo cumbersome government procedures. This requires quick implementation of a new set of technologies, exactly what Cloud Computing is ideal for.

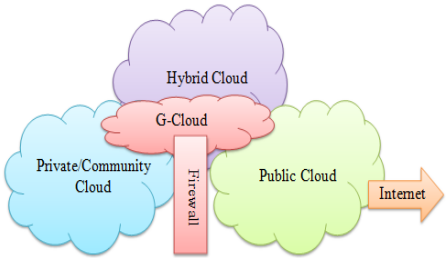

Figure 4: Cloud Deployment Models

G-Cloud, not only provides easily accessible services and scalable resources but also provides many security benefits

like centralized data security, incident response etc which are discussed in the next section.

4. SECURITY BENEFITS OF G -CLOUD

It is always beneficial and economic (cheaper) to implement security resources on large scale and same goes with G-Cloud computing. All kinds of measures put together to defend the cloud infrastructure buys cheaper and same amount of security as doing for a single system. These measures may include strong authentication, secure virtualization and data-filtering; patch management, access control and identity management [5].

4.1 Centralized Data

G-Cloud provides a central data repository which can be accessed ubiquitously with following security benefits:

1. Data leakage diminution: In any enterprise each employee keeps some critical data of the organization with him in his laptop or office computer. This is not a safe practice because this data can be leaked any time by inside intrusion or any outsider. With cloud centralized storage, data is securely stored at a third party location, so local attacks are not possible, unless and until cloud storage is secure.
2. Benefits supervisory: Nowadays companies have their data distributed over different locations instead of a central single location. Thus monitoring of distributed data can prove to be a tedious task i.e. keeping track of which data is where and its statistics. With thin client this can be made easy but cloud gives added fillip of single data repository.

4.2 Incident Response and Forensics

G-Cloud provides read to use resources which can be made available for any incident response or forensics:

1. Ready for forensics: With IaaS cloud service, customer in an organization can build a forensic server which is made ready for use whenever any incident happens. Customer has to pay for the storage when he brings the server online which is one click away from being done. Multiple Virtual Machines (VM) can be used to respond to the incident by distributing copy of the VM to multiple incident responders.
2. Decreased evidence acquisition time: In case one of the servers getting compromised, organization has to just clone the server and make it available to forensic server on the same cloud. No need to maintain unused replicated storage.
3. No or reduced service downtime: With no need of compatibility and hardware issues, there can be reduced or no delay in servicing the fault in server thus reducing service downtime.
4. Eliminate forensic image verification time: While storing the data in cryptographic format, it has to be first converted to encrypted form. To do this the data is applied with hash or other algorithm. In cloud it is not needed as it is already there.
5. Decrease time to access protected documents: Investigations can be sped up by faster testing of candidate passwords.

4.3 Password strength testing (aka cracking)

G-Cloud also provides password strength testing benefits by following means:

1. Cracking time is reduced: To decrease the cracking time for password strength testing practice we can use cloud computing. If password is strong cracking cost will be high.
2. Dedicated machines for cracking activities: Password cracking task can be dedicated to specific machines to keep other workloads separate from cracking. We can limit this activity to non productive machines too.

4.4 Logging

Data logging space requirement cannot be estimated accurately at a particular point of time. G-Cloud provides unlimited and simple data logging methodology and better performance:

1. Unlimited logging space: Logging is often reconsideration, contributing to allotment of insufficient disk space and thus logging is either non-existent or minimal. Cloud Storage changes all this - no more 'guessing' how much storage you need for standard logs.
2. Improved log indexing and search: With your logs in the cloud you can leverage Cloud Compute to index those logs in real-time and get the benefit of instant search results**.** What is different here? The Compute instances can be plumbed in and scale as needed based on the logging load - meaning a true real-time view.
3. Tractability with extended logging: Most modern operating systems offer extended logging in the form of a C2 audit trail. This is rarely enabled for fear of performance degradation and log size. Now you can 'opt-in' easily - if you are willing to pay for the enhanced logging, you can do so. Granular logging makes compliance and investigations easier.

4.5 Better performance

Vendors can create more efficient security software. Cost of cloud is based on computation time or CPU cycles. Therefore cost is inversely proportional to efficiency of software. This will result more efficient security software and such products are rated on the basis of their efficiency.

4.6 Dependable builds

Security can be made inbuilt in the virtualised environment of G-Cloud giving dependable builds:

1. Pre-hardened, change control builds: This is primarily a benefit of virtualization based Cloud Computing. Now you get a chance to start 'secure' (by your own definition). You create your Gold Image VM and clone away. There are ways to do this today with bare-metal OS installs but frequently these require additional 3rd party tools, are time consuming to clone or add yet another agent to each endpoint.
2. Reduce exposure through patching offline: Gold images can be kept up securely kept up to date. Offline VMs can be conveniently patched "off" the network.
3. Easier to test impact of security changes: This is a big one. Spin up a copy of your production environment, implement a security change and test the impact at low cost, with minimal startup time. This is a big deal and removes a major barrier to 'doing' security in production environments.

4.7 Security Testing

G-Cloud reduces cost of security testing. Many organizations share the same software in case of SaaS. They do not need to pay for software. Only computation cost is paid by the users. In case of community multiple organizations share some software which shares there purchasing cost.

5. Security issues in G-cloud

With all these security benefits of G-cloud, it has some security risks too. These issues affect the reliability and dependability of the e-governance services.

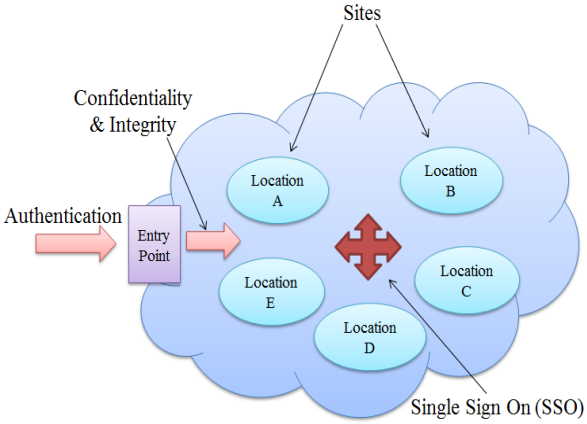

Figure 5: Security Issues in G-cloud

Some of the important security issues are discussed below:

1. Security of data and code: Because we do not know where data is processed outside the user premises, there is always fear of getting data and code compromised while remote execution [7].
2. Physical security: Physical security is concerned with security of data repository or datacenter and processing sites from theft, natural disasters, vandalism, manmade catastrophes, and accidental damages. It also associates to security from intruders or employees. Same cloud resources are used by multiple organizations may create security hazards. We do not know location of resources and how they are allocated [6].
3. Government laws or policies: If data is situated or stored at different countries, it may be seized by government of that country. Every country has its own laws and policies. This may cause loss and compromise of data if the clod provider company is seized, if it comes under any foul activity by other or its own country government [10].
4. Clouds compatibility: If government is using cloud of a particular company and can be interested in transferring to cloud of another company. Condition may occur that two different organizations may takes services of different companies and they may or may not be compatible with each other [9]. Transfer is feasible if both companies are interoperable or compatible with each other. If data is shared between two clouds it must be transferred securely. For example, if Google and Microsoft clouds are not interoperable then we can't transfer our services from one cloud to another.
5. Key management: Key management for encryption must come under the customer's control. But it is not possible for customer to manage keys, because encrypted data is sent when processing takes place which occurs at different locations and this is the function of cloud provider [7]. Security of keys depends on the security of key repositories at cloud.
6. Integrity of data: Because data can be distributed at any locations in the world and is transferred over the internet, one should be concerned with integrity of data. It may be altered in-between the transfer. Man-in-the middle attacks are also possible. We use digital certificates for the integrity of data.
7. Data log: Cloud providers may misuse data logs. Critical information can be passed to unauthorized person or spy agencies who in turn can misuse it. They may store data illegally. Government should have some agreement or policy regarding time period for which data may be stored or logged. They need regular monitoring and auditing of cloud.
8. Vulnerabilities: It refers to the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. End user or cloud systems applications must update themselves regularly. There are many attacks possible by exploring resources vulnerabilities. Vulnerabilities may exist at intrinsic to core cloud computing technology or prevalent in established state-of-art cloud offering [8].
9. Security and audit ability problem regarding VM: Virtual machines are not real systems. They are instantiated and destroyed on the basis of requirements. Once they are destroyed, log is also destroyed. Government should make sure to provide log of processing by virtual machines. The dynamic and fluid nature of virtual machines makes it very difficult to maintain the consistency of security and ensure the audit-ability of records [10].
10. Privacy: Government should allow suing cloud service provider if their personal data is compromised or damaged. Government should commemorate to whom this information is handed over because it may cause security hazards for whole country [10].

6. CONCLUSION AND FUTURE WORK

While restructuring e-Governance on Cloud computing, it brings many benefits like scalability, reliability, cost and storage saving and on demand services etc. With these benefits there also come security advantages too like centralized data, auditing and monitoring, performance improvement and incident response etc. Although these advantages address favorability of this rebuild of e-Governance on cloud, still there are some security issues which must be taken under consideration.

A good deal of research work is progressing, to resolve the security risk of G-Cloud computing like data protection, trust management, virtualization security. In near future, we look forward to resolve these issues and make cloud a secure and more reliable platform for applications like e-Governance.

7. REFERENCES

[1] Marawar, T.R., Kale, S.P., Araspure, K.I., 2010. E Governance. In: DSDE' 10 Proceedings of the 2010 International Conference on Data Storage and Data Engineering, IEEE Computer Society Washington, DC, pp.183-186.

[2] A white paper, e-Governance Solutions and its importance, retrieved online at: <http://www.broadllyne.com/school excel_whitepapers.htm >

[3] Varma, V., 2010. Cloud Computing for E-Governance. Cloud Computing Group, International Institute of Information Technology IIIT, Hyderabad January 2010, retrieved online at: <http://search.iiit.ac.in/uploads /CloudComputingForEGovernance.pdf>

[4] Dillon, T., Chen Wu, Chang, E., 2010. Cloud Computing: Issues and Challenges. In: 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 20-23 April 2010, pp.27-33.

[5] Balding, C., 2008. Assessing the Security Benefits of Cloud Computing. July 21, 2008, retrieved online at: <http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html>

[6] Heare, S., 2001. Data Center Physical Security Checklist. December 1, 2001, retrieved online at: <http://www.sans.org/reading_room/whitepapers/awareness/data-center-physical-security-checklist_416>

[7] Kresimir, P., Zeljko, H., 2010. Cloud computing security issues and challenges. In: MIPRO, Proceedings of the 33rd International Convention, pp.344-349, 24-28 May 2010.

[8] Grobauer, B., Walloschek, T., Stocker, E., 2011. Understanding Cloud Computing Vulnerabilities. Security & Privacy, IEEE , pp.50-57, March-April 2011.

[9] Tripathi, A., Parihar, B., 2011. E-Governance challenges and cloud benefits. IEEE International Conference on Computer Science and Automation Engineering (CSAE), pp.351-354, 10-12 June 2011.

[10] Yang, J., Chen, Z., 2010. Cloud Computing Research and Security Issues. Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on , pp.1-3, 10-12 Dec. 2010.

[11] McEvoy, N., 2011. "G-Cloud Innovation", Cloud Best Practices, GCloudInnovation.com, retrieved online at: <http://cloudbestpractices.files.wordpress.com/2011/05/gcloudinnovation.pdf>