Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Systems Engineering and Informatics

Bachelor Thesis

Analysis of New Technologies for eGovernment Services

Namalgama Mudiyanselage Gayan Damitha Bandara NAMALGAMA

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Department of Information Technologies

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Gayan Damitha Bandara Namalgama Namalgama Mudiyanselage

Informatics

Thesis title

Analysis of new technologies for eGovernment services

Objectives of thesis

The aim of the thesis is to provide an analysis for innovative solution to the public sector services, using a cloud computing model that enables the access of information from the client mobile device.
Partial goals of the thesis are:
- to develop a literature review of current state of online public services and cloud solutions
- to analyse and design a specific mobile electronic public service
- to make evaluation of proposed solution

Methodology

Methodology of the thesis is based on the study and analysis of literature and information sources. Practical part of the thesis will consist of analysis and design of sample mobile application of electronic public service. Methods for software engineering such as Use Case, will be used. The final design will be evaluated with SWOT analysis and compared with other existing applications. Based on literature review and practical part, final conclusions and recommendations will be formulated.

The proposed extent of the thesis

30 – 40 pages

Recommended information sources

Bhatnagar, S. C. Unlocking E-government Potential: Concepts, Cases and Practical Insights. Sage Publications India, 2009, p. 380. ISBN: 9788132102489
Cloud Computing: Principles and Paradigms
Heeks, R. Implementing and Managing eGovernment: An International Text. Sage Publications, 2006, p. 293. ISBN: 9780761967927
ISBN:1118002202, 9781118002209
Volume 87 of Wiley Series on Parallel and Distributed Computing Rajkumar Buyya, James Broberg, Andrzej M. Goscinski

Expected date of thesis defence

2015/06 (June)

The Bachelor Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Electronic approval: 31. 10. 2014	Electronic approval: 11. 11. 2014
Ing. Jiří Vaněk, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Prague on 09. 03. 2015

Declaration

I declare that I have worked on my bachelor thesis titled "Analysis of New Technologies for eGovernment Service" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any third person.

In Prague on 16th March 2015

Gayan Namalgama

Acknowledgement

I would like to thank my Supervisor Ing. Milos Ulman, Ph.D. for all the help and guidance given to me during perparation of this thesis.

Analysis of New Technologies for eGovernment Services

Analýza nových technologií pro elektronické služby eGovernmentu

Summary

The aim of the thesis is to provide an overall view as to how a Cloud computing Model could be implemented within an eGovernment framework, and an analysis as to what type of services or vendors could be used for the successful deployment, for service models, to cloud offerings, and to answer the question as to why Cloud computing should be an essential component of e-Government, and also try to tackle the unique constrains.

Hence we combine the power of eGovernement and mGovernment using the Cloud Computing platform to enhance the relationship between the people and their government, and to ensure that we are minimizing bureaucracy and passing down the cost benefit to the people.

We are trying to cover how these three segments can be combined, and to what extend we could provide a reach to the masses while ensuring the standard protocols are not compromised. While Internet and Wi-fi is becoming increasingly accessible along with the IT literacy. This solution has the ability to mold into any governance need, be it information gathering, economic planing, social-cultural welfare and national security.

Keywords: Cloud computing, eGovernment, mGovernment, mobile technology, SaaS, Hybrid cloud, Platform-as-a-Service, Smartphone

Souhrn

Cílem práce je poskytnout celkový přehled o tom, jak by bylo možné využít Cloud computing modelu v rámci realizace elektronické veřejné správy (e-Government). Práce se také zabývá analýzou typu služeb a dodavatelů, které by mohly být použity pro úspěšné nasazení v produkčním prostředí. Snaží se také odpovědět na otázku, proč by měl být Cloud computing nezbytnou součástí e-Governmentu a jaké jsou jeho výhody a nevýhody. Ukážeme také sílu spojení e-Governementu a m-Governmentu pomocí platformy Cloud computing. Výsledkem by měl být pozitivní dopad na vztah mezi veřejnou správou a občany, a také minimalizace a snížení nákladů na jednotlivé úkony ve prospěch občanů.

Práce se snaží ukázat jak je možné tyto tří segmenty zkombinovat a do jaké míry je možné řešení nasadit mezi širokou veřejnost, za použití standardních protokolů, bez dopadu na jejich bezpečnost. Protože počítačová gramotnost a dostupnost internetu / wifi stále narůstá, má řešení na platformě Cloud computing vysoký potenciál. Samotné řešení je pak možné flexibilně upravovat dle potřeb veřejné správy a nasadit například pro získávání informací, ekonomické plánování, kulturní blaho nebo třeba i národní bezpečnost.

Klíčová slova: Cloud computing, e-Government, elektronická veřejná správa, m-Government, mobilní technologie, SaaS, Hybridní cloud, Platform-as-a-Service, Smartphone

Contents

1 Introduction

The thesis aims to combine technologies such as cloud computing and mGovernment to provide a common platform for all government services. A case study will be taken as an example, which would be the base of designing a new system.

The reason as to why this topic was chose is due to the evolving nature of Mobile usage and the advantages it offers to enhance the already established eGovernment services. Various sources have been quoted as a means of deriving the best practices, and to ensure that the combined experience of studies already conducted would present a strong case for combining such technologies to design a new service, which could be implemented and functional.

Our focus would be on the key aspects of cloud computing and eGovernment, with segments such as approach to implementation methods, security, case studies and designing a new Service, while using the information derived at one point and apply it to another thus cutting short the time between applying for the service and delivery.

Therefore, we have chosen a service that will demonstrate the possibility of implementing the cloud computing platform and incorporating mGovernment with eGovernment, and developing a service which would deliver the benefits of the new technologies in terms of conducting eGovernance.

2 Thesis objective and methodology

2.1 Objectives of thesis

The objective of the thesis is to provide an analysis for innovative solution to the public sector services, using a cloud computing model, that enables the access of information from the clients mobile device.

Partial goals of the thesis are:

- To develop literature review of current state of online public services and cloud solutions.
- The analysis and design of a specific mobile electronic public service.
- And to make evaluation of proposed solution.

Finally the objective is to provide the citizens with a hassle free, on-demand, solution that satisfies the Governments need to deliver better services in a timely manner, and for citizens to obtain those services without wasting time. Cloud Computing has been selected as the best way to address there concerns, and to ensure that we implement a successful Cloud Computing model, we need make sure that we meet the criteria of the ITPOSMO checklist.

2.2 Methodology

Methodology of the thesis is based on the study and analysis of literature and information sources. Practical part of the thesis will consists of analysis and design of sample mobile application of electronic public service. Methods for software engineering such as use case will be done.

The final design will be evaluated with SWOT analysis and compared with other existing applications. Based on literature review and practical part, final conclusions and recommendations will be formulated.

3 Literature Review

3.1 What is eGovernment?

E-Government is not about 'e' but about government. Electronic (or e) government is the process of transformation of the relationships of government with its constituents – the citizens, the business-and between its own organs, through the use of the tools of Information and communications Technology (ICT). The aim is to bring about enhanced access, transparency, accountability and efficiency in the delivery of government information and services.[1]

Even though it is the rapid increase in Internet use that has sparked the recent hopes for “electronic government.” the concept refers not only to more use of IT in the public sector. It is also about governments from several developments, including a general trend to restructure government operations by means of deregulation, outsourcing and competition; the ardent of a cheap, unifying technology standard; and the increasing use of strategic IT tools in business, e.g. Enterprise Resource Planning (EPR), Workflow Management Systems (WMS) and Data Mining tools.

eGovernment is usually presented as using IT to;

- Provide easy access to government information and services to citizens and business
- Increase the quality of services, by increased speed, completeness, process efficiency and other.
- Give citizens opportunities to participate in democratic process of different kinds.

Focus is typically on external services, but one important idea is to use these to make internal operations more efficient, for instance by relying on self-service.[2]

3.2 What is Cloud computing?

[]In a nutshell, cloud computing is a means by which computational power, storage, collaboration infrastructure, business process and applications can be delivered as a utility, that is, a service or collection of services that meet your demands. Since services offered by cloud are akin to a utility, it also means that you pay for wheat you use. If you need extra processing power quickly, it is available for use in an instant. When you've finished with the extra power and revert back to your nominal usage, you will only be billed for the short time that you needed the extra boost.[3]

The essential characteristics that National Institute of Standards and Technology (NIST) definition refers to are as follows:

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick platforms (e.g., mobile phones, tablets, laptops and workstations).

Resource pooling. The provider’s computing resources are pooled to serve multiple consumers using a multi-
tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction(e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.[4]

3.3 What is mGovernment?

Several factors affect the success of smart devices in the markets. The factors include: enhanced processing power of CPUs, GPUs, and the integration of sensors and cameras. Moreover, the success is fostered by the development of highly sophisticated operating systems, the introduction of application stores, the high speed Internet access, GUI, and the multi-touch user interface. The combination of these technologies enables a broad range of applications that cover every aspect of daily life ranging from casual gaming to powerful business related applications.[5]

[]There are plenty of new applications that are used by citizens world over using their mobile phones. One such application is www.citysourced.com which is a real time mobile civic engagement platform. It is a intuitive platform where citizens can identify civic issues (public safety, quality of life, environmental issues etc. and report them to city hall for quick real action.

There are many example of this sort that are growing daily in every city, to provide means of better governance. Therefore we intent to incorporate this methodology to our eGovernment platform using Cloud computing. The citizens can also receive updates about the latest developments and emergencies from the departments they sign-up.

3.4 E-Government Benefits

Government will in turn have benefits in its functions such as

law and policy making

ICTs, especially the Internet, enable gathering of model legislations and policies at international and national levels on any subject, and the experience of nations and regions in the implementation of those laws and policies. It is therefore possible to formulate new policies or modify/review existing laws and policies in a quicker time frame and in a more informed manner.

> E-government, implemented extensively over a period, generates enough data and MIS (Management Information System) that enable policy makers in better decision-making.

One of the prerequisites of a successful implementation of e-government is undertaking an exercise in government process transformation. This transformation can happen only through an exhaustive reform of the legal and administrative framework, e-government, therefore can be a powerful catalyst for legal reform.[1]

Regulation

The regulatory responsibilities of the government arise out of laws. The following areas of regulation can immensely benefit from e-government initiatives:

Statutory registrations of companies and business under various laws

- Taxation
- Environmental regulations
- Police
- Transportation
- Health care
- Education
- Food and agriculture
- Industry and commerce.

Benefits in the regulatory areas could be in one or more of the following forms:

- Better compliance due to stringent tracking and monitoring systems.
- Better revenues
- Better coordination between related regulatory agencies (e.g. police and transportation) due to shared database.
- More transparency in enforcement of laws

3.5 ITPOSMO

To ensure that we meet certain a criteria, we will follow the ITPOSMO concept, to counter the design-reality gap.

ITPOSMO stands for:-
citation
Information: The formal information held by the digital system and the informal information used by the people involved in the system.

Technology: Mainly focuses on digital IT but can also cover other information handling technologies such as paper or analogue telephones.

Processes: The activities undertaken by the relevant stakeholders for whom the e-government system operates, both information-related processes and broader business process.

Objectives and values: Often the most important dimension since the *objectives* component covers issues of self-interest and organizational politics, and can even be see to incorporate formal organizational strategies; the *values* components covers culture: what stakeholders feel are the right and wrong ways to do things.

Staffing and skills: Covers the number of staff involved with the e-government system, and the competencies of those staff and other users.

Management systems and structures: The overall management systems required to organize operation and use of the e-government system, plus the way in which stakeholder agencies/groups are structured, both formally and informally.

Other resources: Principally, the time and money required to implement and operate the e-government system.

This ITPOSMO checklist can be used for describing and understanding any e-government system and stakeholder organizational context.

Outside world: The political, economic, social-cultural, technological and legal factors that impinge on the relevant e-government stakeholders.[6]

3.6 Approaches to eGovernment Management

In terms of implementing the right processes we could consider many 3 key aspect of approaching the procedures in running the government platform. These are Centralized, Decentralized and Hybrid solutions.

Centralized structure allows decisions to be made at the most senior levels. This is a top down approach which means the if the lower level employees are not contributing their insights the system could face usability issues, which if not looked into could evolve into a major risk for the its existence.

Decentralized structure enables decisions to be made at the mid-level or lower level, which means issues are noted and could be taken care of as and when it occurs; typically by individual work units within the organization or even by individual staff. The latter may also be referred to as *end-user computing,* where the individuals within the public sector who make use of the outputs from e-government systems (the internal end users) are also those who operate and/or develop and/or manage those systems.

Hybrid: Decisions are taken at *both* senior and lower levels, either separately or in an integrated manner. This approach is called *federal* or *federated* in some governments.[6]

3.7 Potential benefits of a **Centralized** Approach.

Many public sector organizations began their 'computing careers' by adopting a centralized approach, and there are continuing drives to maintain centralization. The growth of IT in the public sector means increasing expenditure within a political environment that often prioritizes cost-cutting. Centralized approaches are then attractive because they promise opportunities for reducing costs [6]

Achievement of scale economics: Centralized approaches allow most activities to be undertaken more cheaply per unit. Items purchased externally – computers, software packages, consumables, staff training, systems development, consulting and so on – can be decided upon once and then bought in greater bulk. Activities undertaken internally – from system development to implementation and maintenance, and management of all these processes – cover a greater number of staff.

Avoidance of duplication: One main intention of centralized approaches is to have a single version of any particular e-government system for the whole organization, and to store any item of data once and only once. As a result, there is no wasted effort, no wasted storage capacity, and no inconsistency of data.

For example, when dealing with information each persons name and details are captured just once for use on a single, shared database. If these details change or if the required data structure changes, only one set of amendments needs to be made. The database represents the single authoritative source of digital information in the organization. [6]

Sharing resources: A well-planned centralized system holds data used across the organization in one place, allowing all staff to access it. This makes it cheaper, faster and easier to undertake organization-wide activities. Central planning and operation also allows compatible technological and skills to be introduced. Exchange of hardware, software and staff between organizational systems and units therefore becomes much easier and less costly.

However this approach has disadvantages as well. Since everything is centralized the mid and lower level employees who spot various issues cannot take action themselves without the approval of the senior management, who might not understand the complexities related to the issue.

Inflexibility

The greater the amount of central planning that has gone into an eGovernment system decision, and the longer that decision is therefore intended to provide guidance for the organization, the less flexibility it offers the organization to cope with differences between local units, or with internal or external changes. Yet the pace of environmental changes is continuously increasing for public sector organizations as technology, society, the legal framework, and so on, change.[6]

Increased Dependence and Vulnerability
In general, centralized approaches to e-government systems make public sector organizations more dependent and more vulnerable since they create greater numbers of staff and clients relying on single management units, and greater reliance on a few key staff who plan, develop and run e-government. [6]

Potential benefits of a **Decentralized** Approach.

Localization of data means the relevant office has the authority to manage, manipulate and configuring data. It also means that the data that is held is separated from other departments which means the information is not stored in a pool, thus giving it more security and privacy.

Furthermore, issues can be easily identified and remedial measures could be taken faster than having to take various approvals.

Greater Fit between Systems and Local Needs

The closer the proximity of user and developer, the less the communication gap and the more likely it is that the developed system meets the users real needs. External client users have yet to be employed as system developers, but internal users of both internal and external eGovernment systems are being allowed to develop such systems.

Constrain to Decentralized Approach

Barriers to Sharing Database Decentralized approaches can create e-government systems in different work units that are mutually incompatible. The resulting electronic concrete, like its centralized counterpart, constrains the activities that public agencies can undertake or imposes substantial additional time and financial costs on those activities. In particular, strategic, organization-wide activities are constrained. This can lead to anything from a difficulty in aggregating basic financial information across the organization, to an inability to implement any strategic plans, including the delivery of one-stop services for external clients.[quote pg 26]

Barriers to Sharing Other Resources,
including Human Resources

There may also be an inability to share other resources if work units are allowed to set up their own separate e-government systems. It may be hard to exchange hardware and software. Perhaps more importantly, each individual system requires a unique set of skills for system development, implementation and operation. This makes it more difficult to over between different eGovernment systems.

Duplication of Effort
apart from constrained what public organizations can do, decentralized approaches also tend to be very costly because units will often duplicate what others are doing, as those in the FBI, INS and other agencies did. [pg26]

Potential Benefits of **Hybrid** Approach

The most common hybrid computing architecture is the client/server model, in which computing power is divided between the central servers and the local client workstations. This architecture has now been adopted by vast numbers of public sector organizations worldwide.

The underlying networks are also part of the IT architecture. Persuading individual departments to join centralized networks has some way by the central IT unit. This may involve central guidelines on anything from development methods to data structures, or central testing of programs or documentation. This approach was used when the city government in Boulder, Colorado created a new eGovernment system to support building and construction licensing and inspection.[6]

When purchasing equipment for example, it easier for the central government to arrange contracts that will bring benefits such as discounts and more clout in negotiations, in purchasing servers or network hardware, and could provide to other decentralized units a list of recommended vendors, that can be trusted with security and reliability.

This could also lead to resource utilization efficiency in terms of using a pool of resources and sharing of other information within the intra-governmental system, including the budgets, technical know-how etc.

Furthermore, maintaining the entire system would be much more simpler as the identification of issues could be pinpointed to where it started, and a degree of autonomy for govt. departments that engage in totally different services will be able to focus on their side of the system.

3.10 Service Models

IaaS (Infrastructure as a Service)

IaaS is usually the lowest level service available to a cloud computing consumer and provides controlled access to a virtual infrastructure upon which operating systems and application software can be deployed. This can be seen as a natural extension of an existing hardware provision, without the hassle and expense of buying and managing the hardware. As such, there is no control over the physical hardware, but the consumer retains control over operating system parameters and some aspects of security. There is a trend emerging for 'bare metal' services, where access to the hardware at its most basic is provided, but this is more akin to traditional data center or 'hosting' services. For the majority of potential cloud consumers, there is a desire to move away from as much of the detail as possible and therefore progress upwards through the cloud service model stack.

Platform as a Service (PaaS)

Platform as a Service (PaaS) sits atop IaaS. This layer is ready for applications to be deployed, as the necessary operating system and platform-related tools such as language compilers are already installed and managed by the cloud computing provider. Consumers may be able to extend the existing development platforms installed upon them. The key difference with cloud computing in this case, however, is the rapid provisioning or elasticity; classic web hosting relied upon manual management of provisioning and therefore required human intervention if demand increased or decreased.

Software as a Service (SaaS)
Finally (for the NIST definition), there is Software as a Service (SaaS). This service model abstracts the consumer away from any infrastructure or platform level detail by concentrating upon the application level. Applications are available via thin client interfaces such as Internet browsers or program interfaces such as mobile phone apps. Google's Gmail is one popular example of a cloud computing application. An organization can adopt Gmail and never concern itself with hardware maintenance, uptime, security patching or even infrastructure management. The consumer can control parameters within the software to configure specific aspects, but such interventions are managed through the interface management. The consumer can control parameters within the software to configure specific aspects, but such interventions are managed through the interface of the application. The end user gets an email service and does not worry as to how it is provided.[3]

3.11 Deployment Models

A public cloud, as its name implies, is available to the general public and is managed by an organization. The organization may be a business (such as Google), academic or a government department. The cloud computing provider owns and manages the cloud infrastructure. The existence of many different consumers within one cloud architecture is referred to as a multi-tenancy model.

Conversely, a private cloud has an exclusive purpose for a particular organization. The cloud resources many be located on or off premise and could be owned and managed by the consuming organization or a third party. This may be an example of of an organization who has decided to adopt the infrastructure cost-saving potential of a visualized architecture on top of existing hardware.
The organization feels unable to remotely host their data, so they're looking to the cloud to improve their resource utilization and automate the management of such resources. Alternatively an organization may wish to extend its current IT capability by using an exclusive, private cloud that is remotely accessible and provisioned by a third party.

Such an organization may feel uncomfortable with their data being held alongside a potential competitor's data in the multi-tenancy model.

Community clouds are a model of cloud computing where the resourcing exists for a number of parties who have a shared interest or cause. This model is very similar to the single-purpose grids that collaborating research and academic organizations have created to conducted large-scale scientific experiments (e-science). The cloud is owned and manged by one or more of the collaborators in the community, and it may exist either on or off premise.

Hybrid cloud are formed when more than one type of cloud infrastructure is utilized for a particular situation. For instance, an organization may utilize a public cloud for some aspect of its business, yet also have a private cloud on premise for data that is sensitive. As organizations start to exploit cloud service models, it is increasingly likely that a hybrid model is adopted as the specific characteristics of each of the different service models are harnessed. The key enabler here is the open standards by which data and applications are implemented.[3]

Therefore, we could conveniently choose the Hybrid methodology for deploying our eGovt platform, as we only want to have a system where the user can only upload information and access output, whereas the relevant govt. dept will have the full access to manipulate, configure and accessing capacity.

3.12 Risks

As with any new approach or technology, there are limits by which benefits can be realized, and a new way of working may introduce additional risks. Cloud computing is no different in this respect, particularly as the model is still maturing.

From a consumer's perspective there is a great deal of focus upon security and trust. Many users are ambivalent about where 'their' data is stored, whereas other users (specifically organizations) are more sceptical about delegating the location of the data along with the management process that go with it.

For many smaller organizations, the cloud computing providers will be bringing enterprise-level security to the masses as part of the offering. Most private individuals and small businesses are unaware of the risks of lost data and the adverse impact that it can have upon daily operations. As a consequence, it is likely that they have not put the appropriate security measures in place. In this case, a move towards the cloud can bring real benefits.

The use of third-party services potentially introduces security and privacy risks, which may therefore require an additional audited overhead if the services are to be successfully and reliably trusted.

Another concern is that of vendor lock-in. If an organization utilities IaaS, it may find that the platforms and applications that it builds upon this service cannot be transferred to another cloud computing that it builds upon this service cannot be transferred to another cloud computing provider. Similarly, services at PaaS and SaaS can also introduce nonstandard ways of storing and accessing data, making data or application portability problematic.[3]

3.13 In our own solution

Risks are mostly associated with the security issues and managing such a large quantity of data. Therefore we must focus on implementing a fool proof mechanism to avoid this tenancy.

Security and Privacy will be maintained since we do not plan to outsource data management and infrastructure to a third party. We will ensure that only the a limited amount of employees have access to stored information. The will be highly sort after individuals. There will always be a duplicate copy stored and 2 factor authentication is necessary to delete or edit data.

3.14 Security

[]Security of what?
Security is all about safeguarding the ICT assets of an organization. The assets in the portfolio could be internal assets of the organization or external assets. While the internal assets are easy enough to visualize, the external assets that lie outside the 'perimeter' of the organization include the assets of the clients, remote users and business partners who need to communicate and collaborate with the organization day in and day out. The ICT assets themselves can be of a wide variety including the following:-

Data in the form of data on the organization, its transactions, sensitive data relating to citizens and businesses such as the socio-economic data of citizens and business returns, data relating to properties of individuals and their titles and charges thereon, medical data of citizens, data of educational institutions and social security data. The data can be in individual databases, data marts or in data warehouses.

Information in the form of processed data, such as processed tax returns, driving licenses, medical claims, annual business returns, we sites of agencies, directories of users, work flow processes etc.

Knowledge resources, e.g. patents, Acts Rules and Regulations, research papers, reports, meta data schema's, standards and specifications, most of which may contain valuable intellectual properties.

Programs such as e-government applications that provide services to millions of citizens and thousands of businesses, operating systems, email systems and web servers. Most of them contain thousands of person years of efforts behind them.

Hardware such as PCs, servers, routers, switches, data centers.

Networks e.g. LANs, WANs and wireless networks.

Security against What?
The threat to security of ITC systems may come from many sources and in many forms. It is necessary to identify these threats, in the context of a particular e-government project or of the environment in general. What are the sources of threat to e-government? The source can be internal or external to the government agency.

Internal Sources of Threat
Government employees working within e-government projects may misuse their access privileges to secure financial gains or disgruntled employees may try to sabotage the program to spite the government and/or to retain their vested interests.

Employees of the private partners of e-government operating the systems in a PPP arrangement may resort to such a misuse as above.

Customers of the e-government programs may attempt to access the databases for financial gains.
External Sources of Threat

Professional hackers who have the requisite technical skills to break into e-government systems, are perhaps the biggest threat. They may not expect any financial or other gains but the sadistic pleasure of disrupting citizen services.

Criminal organizations which are inimical to the government.

Terrorist organizations that want to destabilize economies predominantly depend on digital systems.

Intelligence and investigation agencies that want to secure sensitive and classified information from government agencies.

What are the Types of Threats?
Threats to ICT assets may be different types and of varying intensities and impact values. As a corollary, the attacks on security of system can be in different forms including the following:

Defacing of web sites and filing the home pages with objectionable material.

Hacking into servers and stealing valuable data and information.

Damage to critical databases and applications.

Denial of Services Attack (DSA), which involves flooding the government portals with millions of requests at business-critical hours to deny the service of genuine users.

Virus attack directed against a particular government agency or broadcast without direction, which may have the effect of corrupting data or application programs and is usually associated with slowing down or even breakdown of networks.

The damage to ICT assets need not always be a result of such malicious attacks as above. It can be occasioned by accident through inadvertent, incorrect usage of the systems of mandatory combination of alpha-numeric and special characters, life period of a password that forces users to change the password, restriction on adopting the same password time and again and procedures for revocation of password.

(b) It is advisable that the directory be maintained securely and centrally so that it is available to all authorized users.

(c) Lightweight Directory Access Protocol (LDAPv3) compliance is preferable when a very strong security is not required.

(d) Implement a fault-tolerant solution that provides 24 X 7 availability of directory services.

(e) Design and use a meta data schema together with a taxonomy that prescribes what information of the person is registered and in what uniform format and what are the classes of users and their hierarchies . Omission in this regard could leas to a serious confusion in the registration and retrieval process as the e-government systems scale up to a few thousand users.

Access Management Systems
An Access Management System serves the following objectives:

It enables ICT systems to identity the user uniquely by matching the password, digital identity token or other device that carries the digital identity of the user with that registered in the system.

It authorizes the user to perform only those tasks and transactions that are predefined as per the privileges granted by the system administrator at the time of registration or subsequently.
3. It can maintain intelligence of users who try unauthorized access of tasks for which they are not privileged. This would be available to the management for review and remedy.

Access Control Lists (ACLs) and Advanced Access Control Lists are industry standards in this area.

Interaction Management Systems
The objective of interaction management are by far the most comprehensive and complex. They include assurance of the following principles of a comprehensive security, which are, in a way, the founding pillars of interaction management.

1. **Authentication** or the assurance that the user is actually the person who he or she claims to be.

2. **Integrity** or the assurance that the message or document sent or transaction effected through an ICT system has not been tampered with, traveled from source to destination safely and got stored their in securely.

3. **Confidentiality** or the assurance that the content of the message or document sent or transaction effected has not been read by anyone else except the person to whom it has been sent.

4. **Non-repudiation** or the assurance that the person who has transacted shall not repudiate the same at a later date.

The above four axioms are fundamental to a secure digital environment and flourishing of e-government transactions. These are more significant for the e-government scenario because these four requisites are precisely, needed for a whole gamut of e-government transactions involving exchange of contracts, title deeds, issue of statutory certificates, financial transaction, filing of tax returns, approvals and sanctions accorded through a workflow, etc. PKI is a mechanism that gives all the four assurances.

Tools for User Management
Username and Password system is the conventional system of user management. It has several security issues. The user can compromise the password. The password can be hacked. The password can be transferred. It does not assure that the person keying in the password is the real-world person to whim it was assigned.
A **digital identity token** is a popularly used device to overcome some of the shortcomings of a simple password. It is a photo ID card that also has the password embedded in it either magnetically or as a chip. It serves the dual purpose of controlling the physical

access to the work premises and of controlling access to the ICT systems that the user is authorized to access. It is quite suitable for employees in corporate work environments. The digital identity token is not completely foolproof or transfer-proof because it depends on human intervention at the entry through verification of the photo ID with the person's face.

A **biometric device** seeks to overcome the deficiencies of a token by using the physical features of a person, such as the fingerprint or iris to establish identity uniquely. These features are captured at the of registration, converted into a code using certain algorithms and stored for comparison at the time of authentication. The biometrics field is still in an evolutionary stage. We have biometric mouse and biometric verification devices attached to PC or permitting access into hight security areas.

Public Key Infrastructure (PKI) is a technology that is based on the theory of cryptography or converting an intelligible text or digital content into a form that can be decrypted and read by the user or person to whom it is sent, PKI basically uses the concepts of Digital Signature Certificate. Asymmetric Key Pair, Public Key, Private Key, Digital Signature and Encryption. [1]

4 Own Solution

4.1 From the applicants perspective

- Confirmation and a tracking number is sent to the user to track his application, so that the user is aware about the submission request.

- The applicant must enter his National Identity Number or equivalent of his Social Security Number or when submitting the form.

- A digital signature might also be requested according to the circumstance.

4.2 From the Governments perspective

In terms of dealing with a large pool of information (Big Data), it's security been an obligation of the data holder, the govt could implement a few key security aspects towards this end.

- Access layers
A clear guideline and a Code of Conduct must be established among the govt. employees. It should be noted that not everyone should have access to data, and if possible a data segregation mechanism should be established. This means, a certain department can only access data that is required only. Data obtained should be concise and relevant.

The number of employees having access to this data should be limited. Certain passwords in terms of logging into the cloud application should be maintain, including a log book.

- Encryption of data
Data could be encrypted and should be considered a part of the cloud. Techniques such as attribute based encryption may be necessary to protect sensitive data and apply access controls.[7]

- Security information and event management
[]A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it’s important that the SIEM administrator first creates a profile of the system under normal event conditions.[8]

Intrusion detection (ID)

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network. (attacks from within the organization).

Intrusion detection functions include:

❿ Monitoring and analyzing both user and system activities
❿ Analyzing system configurations and vulnerabilities
❿ Assessing system and file integrity
❿ Ability to recognize patterns typical of attacks
❿ Analysis of abnormal activity patterns
❿ Tracking user policy violations

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the *passive* component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the *active* component: mechanisms are set in place to reenact known methods of attack and to record system responses.

In 1998, ICSA.net, a leading security assurance organization, formed the Intrusion Detection Systems Consortium (IDSC) as an open forum for ID product developers with the aim of disseminating information to the end user and developing industry standards.[8]

We will implement will be isolated from the client by using the **Brokered Cloud Storage Access.** In order to facilitate this concept two services will be created.

- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

Once an client as sent the form, the officials at the department, who in-turn sends a data request to a proxy's external service request.

The proxy forwards the request to the broker.

The broker requests the data from the cloud storage system.

The cloud storage system returns the data to the broker.

The broker returns the data to proxy.

Finally the proxy sends the data to the client.

Furthermore, the building containing the servers should have enhanced access security, along with finger printing, infrared detection, CCTV cameras, security personal etc.

4.3 Solution explained

In the solution, we have incorporated the technologies for the eGovernment platform, using Cloud Computing, mGovernment where the government could provide an essential service to their citizens.

We have analyzed the technologies involved from the perspective of the front-end and the back-end as to how the layers of access could be implemented, and the security required to ensure that data is encrypted and protected.

The solution meets the criteria placed by ITPOSMO, and takes into consideration the SWOT Analysis, and CATWOE methodologies.
We have focused on the types of deployment available and have gone ahead with choosing a Hybrid platform to cater to our own needs and to add an extra layer of security using a Brokered Cloud Storage method.

The Cloud based Passport Issuing Service is an ideal service which could be useful in providing a service to people who are already away from the country, and would be in need of assistance to provide a safe return home without being withheld by law enforcement in their host country, as the host country might have strict laws that could jeopardize the safety of foreign national without travel papers.

Furthermore, the system is secure, and is a powerful tool in storing, retrieving and manipulating information to a complex and cumbersome process, such as issuing a new passport.

For example suppose an individual wants to apply for a new passport. Following are the steps that he/she will need to take to get in done without even leaving his/her house or office. Usually the applicant has to visit the office in person, and more than once.

The system we plan to implement enables to possibility for the individual to use their mobile device and log on the website, and fill in the necessary form and click 'apply'.

This solution is based on the intention that the entire govt. system will be connected to a cloud. This is only a brief example of what could be achieved if such an e-government system based on a Cloud computing platform is available.

4.4 A scenario that explains the benefits of the solution

Suppose a student or traveller abroad runs out of pages or losses his/her passport the normal procedure would be to go to the Foreign Police and report the loss. In case of running out of pages, it means going to the nearest embassy to apply for a new passport.

This obviously requires a lot of time and money. Not to mention the delays and the red tape that must be dealt with.

With the new system the student/traveller can go to any cafe or log in to the Wi-Fi, go on the Internet using a PC or remote mobile device, and log into the passport office website using their old passport no./ National ID no. and fill in a form with all the details, after which the credit card number could be entered for payment for the service.

After which the applicant can submit this information, and the Passport Office which has all the necessary access to the relevant information, could authenticate and there by approve a new passport, and mail it to the country where the student/traveller is located.

This can happen within a few days and the user can collect the new passport from the nearest post office by showing the proof of identity.

This piece of identity could be their National ID card or a tracking number which could be displayed to the post office counter.

4.5 Benefits of the new system based on a SWOT Analysis

A **SWOT Analysis** format can be done to demonstrate the implications to the stakeholders of the system. The points listed are a combination of available resources and the authors own observation.

Strengths (for eCitizens)
a. Citizens to not have to travel to government offices, which in turn can bring benefits such as

- **less transport costs** – the user doesn't have to take a day off to travel to the government passport office. Now he/she could get it done 24hrs a day, as long as there is a mobile device and an Internet connection.
- **reducing the loss of productivity** – time spent on the road, and in waiting rooms is finally over.
- **reduces the need for governments to have branches covering different geographical locations** - with the increase in mobile penetration and access to smart phones and Internet connection; citizens from even the remotest village can now access govt. services.
- **Up-to-date and relevant information** - citizens can update their information to the cloud, which in turn helps the government to have relevant, up-to-date information (even for statistical purposes),
- **less need for employees** by Govt. departments in fact interaction is brought down to a bare minimum.
- **cost benefits to the public**, in terms of reduced overheads and salaries for bureaucrats, incurred by the government.

➓ **Keeping track of their application remotely** - enables comprehension and clarity of the entire process.

(for Government)

- **No need to maintain outdated methods to store and update data** - maintaining files and cabinets and other archives could be tedious and costly,
- **easy retrieval of data**,
- **overall increase in national productivity** (through Government efficiency),
- public will feel much more closer to their government,
- **data/information could be shared across various ministries, departments etc.**
- funds saved from spending on the public sector workers could be reduced, thus allocation of money to much more important tasks achieved,
- long-term benefits such as monitoring peoples behavioral patters could be measured by high end mathematical software, which in turn helps in planing and organizing, (e.g online daily registration of new born can be accounted annually, and directly used to extrapolate population planning),
- integration of services will be possible with an addition on new services layers in the future,

Weaknesses

- information gathering could be time consuming,
- not every member of the society is IT literate,
- disable people might find technology usage an issue,
- legislation relating to Information Security should be enacted and implemented,
- proper measures should be taken to ensure the system is always activated,
- data or information provided by a user should be checked against authenticity,
- initial outlay could be costly, and not all governments are tech savvy,

Opportunities

- services could be expanded using the same data, for another service request,
- cash free payment methods could be implemented with the help of mobile phone operators, thus bring increased revenue to the government, and bring down low level corruption,
- services such as tax payments could be streamlined, and used to cover a wide geographical area, thus widening the tax net, and bring more revenue to the government,
- services could be requested by citizens even while they are holidaying abroad, without the need to make visits to their embassies more than once,
- in the future, even elections and national polls could be done via mobile devices, and results released much earlier,
- could also be used to implement and influence policy making, thus gathering input from the grassroots level of the population,

Threats

- data centers or server farms should be protected from natural and made made disasters,
- data gathered should meet the Information Act, and necessary legislation, or else there is a threat that activists and the citizens themselves, would protest against their invasion of privacy,

- relevant security checks must be implemented to double-check if indeed an individual as requested a services (such as a new passport), - this could be done with the regional law enforcement, and using other security checks like text messages with security codes sent to the users mobile number,

4.6 Implementation based on ITPOSMO model

Factors to consider will be done under the **ITPOSMO** guidelines

Information – will be stored in such a way that the stored information will could also be used as a template for future expansion of public services. For example the Name, DOB, and the Residence address will form the initial layout of the information template.

Technology – the input of data will be done using an interface that is compatible with the iOS and Android devices. Files such as various paper documents from the local authority can also be uploaded and archived. There is also an option of using a the camera of the device and upload the image file into the archive. This archive is also a part of the Cloud.

Process – once a new document is uploaded or updated, a relevant government department is notified. The user has the option of choosing to which department it should be forwarded to. This could be done in a tag. The system has a database of a limited Government departments.

For example:- a user uploads an image of a paper form in to the Cloud, and tags the relevant department name. Then the departments IT division gets a pop notification, and the relevant officer views the document and archives it and sends a message to the mobile phone that the document has been successfully received.

Likewise the user could also use his information which is already in the Cloud as a template to fill online application forms.

The update information could be accessed by various Government departments with the permission of the individual who's information they need to analyze.

Objectives and Values - the primary objective is to have a more organized, easily accessible, consistent and a secure approach to managing and storing big data. The stakeholders involved should benefit at both ends by ensuring up-to-date information is stored, thus adhering to the principles of data laws. The data obtained could be used for approximation, in terms of future planning of infrastructure, through adequate allocation of resources.

For e.g a registration in number of offenders means there is a need for more policing of a certain community. Or another example could be the registration of new birth certificates on the platform could easily allow the Govt. to estimate population growth and have a more up-to-date figure on these indicators.

4.7 Designing of the New System Based on the CIPSODA concept

Capture of data is done when the user loads the page with the form and fills it. The form has all the necessary fields needed by the department to process any request.

Input An form that has a responsive design format and is therefore possible to be viewed in any mobile device, be it a phone or a tablet. The user also has the option of downloading this information to his phone/tablet to be filled later. The user also has the added option of getting a print out later on.

After the form is filled the user selects the “send” button. In order to provide a degree of security and authenticity, the user has to input his NID (National ID no./Social Security No. etc)

Furthermore, the user will receive a text message into his email and phone, with an application tracking number.

Process The data which is sent to the govt can be altered by selecting the right options available at the web page. A user interface designed to support this process will be built, with sliding options and as well as scrolling options. Furthermore, the user also has an option to change the sent information using the tracking number he receives.
Store: The information sent will be stored in a secure server, which is under strict govt. regulations.

Decision: The govt officials tasked with ensuring all the documents and information sent are in line with the legal procedures can validate the information and process the request. If further information is required, the user can be contacted via SMS or email. The user will thus have time to re-submit or attach further documents to his formal request, using his tracking number.

However if everything is already in order the users request can be approved and decision will be sent via SMS or email.

Action: If the decision is made and the user is not satisfied he/she could make an appeal, and the tracking number could be used as a reference.

In terms of planning there are key things to consider such as Data Security, Budgetary allocations, Type of cloud, Data

4.8 CATWOE

We can conduct a more liberal analysis of our new system through a CATWOE process.

Clients
There are only two stakeholders in this program. The citizens and their government. However at the receiving end would still be the public, as it is them that will make this system a success and increase over all productivity, bring positive externalities.

At the moment people find it extremely difficult to get information regarding, dealing with their government. Thus they have to make numerous phone calls, or visit the relevant govt. office, during a weekday, depriving them of their livelihood, while being a burden to their employer. This in turn reduces the economic productivity of the whole society in terms of aggregate wise.

Since the new system would allow for people to interact with their government, using their mobile devices, it will in turn give a sense of convenience, and at the same time people would feel as if govt. services are right in their pocket.

For e.g. the ability to download a form and fill and upload it to the relevant govt. database would save a lot of paperwork, traveling time and other misplacement of material while helping to cut down on corruption, whiling tracking the application would be more convenient.

In terms of the people who would stand to loose from this new system would be govt. employees who would lack training of new technological deployments. However, since the process is gradual and the social benefits outweigh the negatives while recruiting new IT capable people would mean more employment opportunities.

The other segment that would be affected would be the senior citizens who might not be IT savvy and would have problem with adjustment.

We will engage in reconciling our Objective and Values segment with the **CATWOE** process.

Actors

The employees will be the key component of ensuring that the system functions smoothly, in terms of Administrative, IT support, Security and Database Management.

Regular maintenance checks and attention to any issues should be tackled. This should be done both inside and out, testing the system and UI on a regular basis, to ensure that users have a comprehensive interface and user support will be available on request.

Emphasis will be heavy on the security aspect of the system as vital information will be stored on the database.

Another key actor would be the telecommunications industry which will facilitate new networking technologies such as 3G or 4G spectrum. Since Wi-fi will also be available in diverse locations throughout, there will be more ease of access.

Transformation

The inputs will be from the user. The user can either download, or simply fill in the details on an online form and submit it to be processed. The processing will be done accordingly. If the user lacks any input information necessary for the smooth processing, an email or a text message will be sent to him/her. The user will have a period of time to rectify this error and re-submit the application.

There will also be a method to track the application, and any fees could also be paid through their credit card or through their mobile operator. The steps in between will be done by the relevant officials to ensure that the application is legit, and that all relevant information provided meets the necessary requirement.

The output will be through registered post, or a soft copy depending on the importance and the scenario. The users also have the option of collecting the output at the dept. themselves.

Weltanschauung (Worldview)

In terms of the bigger picture, we want to focus on effective governance and provision of govt. services to the public without a hassle. The entire system should allow the capability to expand and whiling creating an inter-governmental platform to share information about the individuals as and when required.

This will lead to fewer malpractices, and more transparency in the process, rooting out corruption. The other benefit is the overall information could be used to compile more accurate statistics, thus enabling the extrapolation of data for future planning as a government, and could be used as an intra-governmental platform for data sharing and storage.

Furthermore this will also enable better social indicators. For e.g. number of child births in a certain region can help the govt. to allocate, tables and chairs for junior schools.

The system could also lead to better economic indicators and clarity in terms of areas such as paying taxes and registering entities.

This could further enhance the “Right to Information” bills in passed in the legislation.

Owners

The owners will be the govt. which will provide legitimacy for the project and ensure public trust in the system. The information consists of the details of the each and every individual. However the govt. has the obligation to maintain, provide security and other fiduciary responsibilities under the laws of the land, enacted by the parliament.

Environmental constrains

The environment will have a direct benefit as the paperwork will cut down, traveling will reduce, and the only instance where the environment could be affected is if the electricity from the data centers are powered by electricity grids powering them through fossil fuels. While at the same time a proper mechanism should be in place to get rid of the electronic waste that will be an issue if not properly addressed.

Skills and Staffing – with the growth in number of graduates and increased exposure to IT related education being embedded into the education system, we could ensure a steady reserve and availability of talent pool to be recruited into the department.

Our focus is on people who are skilled in IT, such as IT Support, Administrative, Database Management, UI designers and Security Experts.

Even though the salaries for this segment of labor could be higher compared to the other semi-skilled staff, the benefits accrued through cutting down the employees and closing down regional offices would mean that it could be a net gain.

Management System

The system could be managed by a separate IT department with the sole aim of ensuring the reliability of the system. This department will be dedicated towards this purpose to ensure that there is a direct line of communication with a relevant govt. body to represent their issues, be it more funding or other regulatory issues.

This govt. body could be for example the Ministry of IT and Telecommunications or the Ministry of Internal Affairs. Nevertheless, there should be adequate provisions enable to ensure that the person who's data is being used is aware of it and permission should be obtained from that particular individual, other than in circumstances related to National Security.

It is recommended that proper regulatory framework is in place and there is also a case law in order to relate to it when the govt. breaches its obligations.

Other Resources

In terms of other resources we have to consider the cost of implementation. The payment of services, and the long term maintenance cost of the project should be properly analysed. Considering the fact that the return on investment is long-term and the nature of the project itself dictates that it is the government itself that should look into its implementation.

The return on investment could spread over many years. However, there are fees charged anyway to provide services to the public, which come through stamp duties, direct and indirect taxes, and fees charged on paper applications. With the cut down in overheads, such as redundant staff and other overheads like office space and rents, it will no doubt boost the productivity of the state sector.

4.9 Entire Process in steps- How the system works when the user tries to obtain a service

Step 1

eCitizen (User) logs into his smart-phone and goes to the department website.

Step 2

eCitizen fills the form and; attaches the necessary documents and clicks the 'Submit' button.

Step 3

e Citizen then receives a text message and an email along with a '**tracking number'** to be used for keeping a tab on his application process.

Step 4
The e Citizen pays the application fee from his/her mobile phone, using mobile banking or through his service provider.

At the Passport Office

Step 1
The officer in front of the PC gets an alert. He/she clicks on the application and view the request with the form which was filled by the client.

Step2
The Officer then goes through this form and sees if all the necessary details are filled and relevant.

Step 3
If for example a certain record is not attached as per the status quo; the officer opens another application on the same PC and logs into a database (e.g Criminal Record of the Applicant)

Step 4
Once the applicant has a clean criminal record, the process started. Within a few hours approval is done and the applicant get another notification to come and collect his passport in person.

Step 5
Once again the tracking number is used for all verification purposes.

The information of the applicant is stored in a Central Database which has allocated space and access related to the Passport Office.

4.10 Improvement of the process itself can be summarized accordingly

- It is easy to see how quickly the process can take place. With the amount of information available on-demand to the passport officer, and the ability for the e Citizen to apply for a govt. service using is mobile device at anytime of the day at the comfort of his/her home.

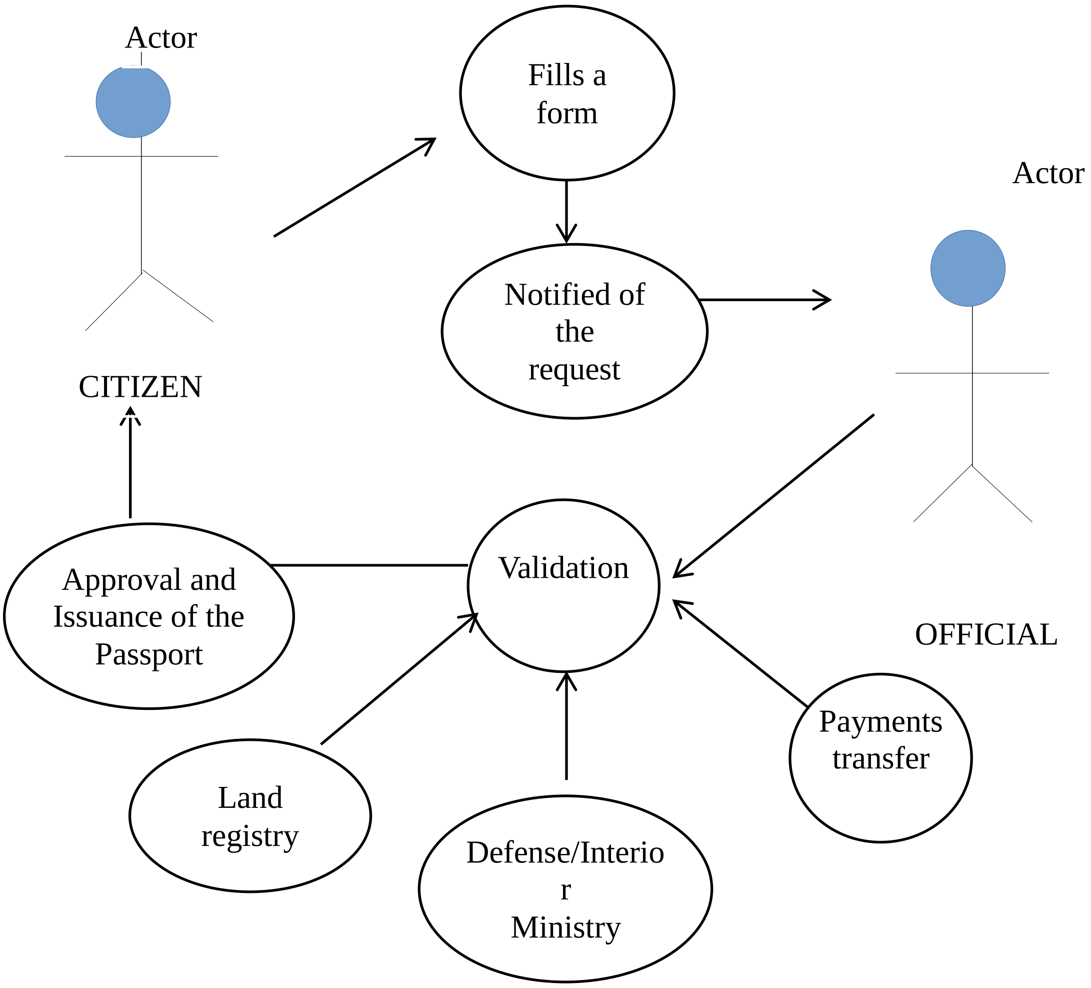
❿ In the above example we saw how easily the officer was able to log into the cloud and find out all the relevant documents and details regarding the applicant for cross examination and fast approval. In real life this take a lot of time and effort.

❿ Imagine if all government departments had this capability, we could really bring eGovernment services to the masses, and receive live feedback. This means the amount of workload is reduce and the government does not have to allocate resources on employing more bureaucrats, except for a few IT capable individuals.

❿ And for the people, they do not have to go anywhere or from pillar-to-post to get their documents done.

4.11 Use case diagram

[Figure 1 Use Case Diagram]



(Source: author, 2015)

4.12 Use Case explained

Submitting of the request

The citizen logs into the website using the mobile phone, and then fills a form. With the submission of the form. The User is identified by his National ID no.

For example if a student or a traveler in a foreign country wants to request a new passport he/she has to go through the cumbersome process of visiting the embassy and going through the bureaucracy.

Instead he/she could use his mobile device; log-in to the Passport Office and fill in a simple application number. After-which the user receives a tracking number via a text message.

The officer receiving the request is used as the 'broker' and forwards the relevant information to the relevant govt. departments. The the officer obtains the relevant information to verify the details as the applicants Date of Birth, Registered Address, Criminal Record, etc. using the information stored in the Cloud.

This obtained information is verified against the information submitted by the applicant during the time of sending the request application. All this could be done within one hour.

After all authentication is confirmed. The officer then issues the passport. The passport is sent to the foreign address of the applicant.

The finally the applicant goes to his closet post office, shows a valid proof of identity document and obtains the passport.

Notification and Validation

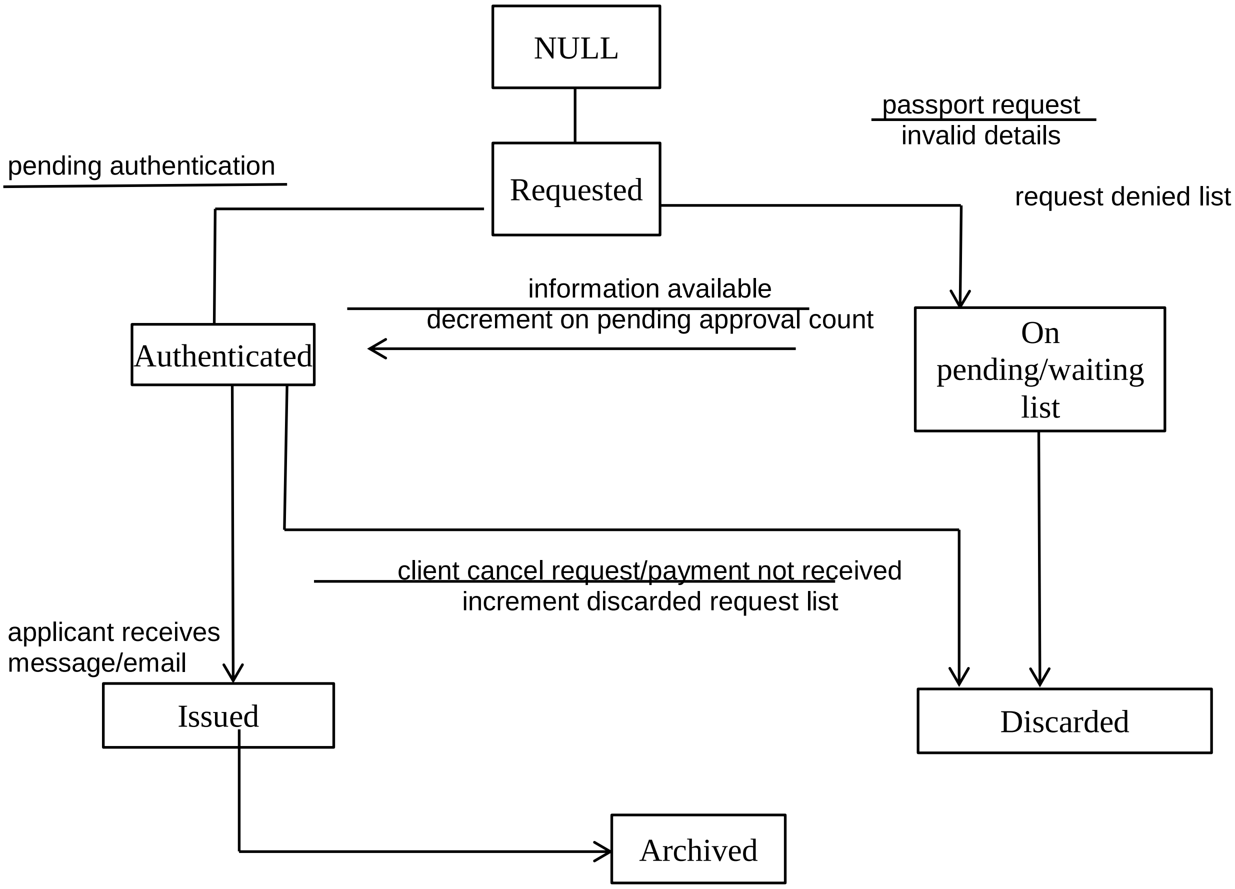
The department in charge of issuing new passports get notified when an applicant has submitted a request. An official in assigned the ticket, and he/she checks the validity, by obtaining information from other line Ministries or departments, to verify the address, DOB, National ID match to those that have been submitted by the Citizen. The validation check is done by the Official through logging into the cloud that stores the information. The official enter their log in and password assigned to them for this purpose.

Approval

Once the information is verified the new passport will be approved and the Citizen gets an email/text message notification.

4.13 State Transition Diagram

[Figure 2 State Transition Diagram]



(Source: author, 2015)

4.14 Maintenance of the New System

A separate government agency will be tasked with the following :-

Data Security and Privacy

The agency will be in charge of taking care of the Data Security using modern software methodologies. They would be tasked with implementing the required protocols based on Big Data Security, such as Access Control, Auditing, Authentication and Authorization.

Training and Recruitment of skills and manpower.

The staff that needs to be trained will be identified. A background check would be done with the help of national intelligence agencies. Recruitment on the basis of experience, Technical know-how, and creating relevant designations based on their requirement will be done by this agency.

Procurement of equipment and other infrastructure through:-

- technical evaluation to find out the best practices in the industry, to learn and enhance tailor made solutions through research.
- industry experience
- public-private partnerships (PPP) will be done to implement the necessary tools.
- carrying out a competitive bidding process

Coordinate between the relevant ministries and departments.

As a coordinating agency between the Ministries and departments in terms of “Cloud” related matters, such as submitting budget proposals and secure access to funding.

Repairs and troubleshooting and provide basic training for system administration

A rapid response team should be set-up to ensure round the clock maintenance and to analyze and protect data against theft and attacks. A complaints division will also be setup to receive public inputs on issues related to functioning and troubleshooting.

4.15 Re-Evaluation of the purpose of the system

- **Share intra-governmental data and information for on-demand accessibility.**
  (e.g passport dept. requesting the internal affairs for a police report on an applicant) Department employees can obtain relevant documents needed to approve a request by simply sharing information and other relevant details. A request could be sent to a sister department. Intra-governmental communication could prevent fraud, and increase efficiency.

- **To avoid the public going from pillar-to-post to obtain govt services.**
  People do not have to go from one department to another collecting documents and paperwork to get approvals. The concept of one-stop-shop can be applied while obtaining government services.

- **Increased efficiency, safety, reliability, speed and productivity.**
  Government resources are not wasted with employing excessive staff. Instead a few well trained staff could do more work in less time. Furthermore the govt. doesn't have to open branches countrywide anymore. These benefits could be passed

down to the citizens in terms of lower taxes and less overhead costs.

People also benefit in terms of more interaction and up-to-date information stored about them by the govt. For example this could be beneficial in areas such as taxation. The revenue input could be used to automatically calculate the relevant tax, according to the tax base and bracket.

- **To create a pool of resources to tap into information**

The relevance of information relies on who up-to-date and concise it is. To maintain this data, the govt has to spend much on research, census and statistical gathering mechanisms. Furthermore, accessing of files have never been easier. And sharing them among relevant institutions have opened other avenues.

- file storage

Up-to-date information stored in a database is more accessible that what is stored in files and other furniture. This results in some important documents getting misplaced and leaked.

- more coordination between govt. departments

more coordination means a more efficient govt. A three-way coordination among govt. departments and the citizens means that the departments become more service oriented.

- sharing information

this is an important part of the system. Corruption and fraud could be identified and evidence could be easily produced, in terms of back tracking data.
Furthermore, govt. employees can now request various documents among a host of departments. For example the tax department can request details of a company from the registrar of companies, and the social office, or even the labour department.

- **To act platform connecting mGovernment, Internet banking, Mobile payments**
  In terms of using new technologies for eGovernment, we must look at a way to combine Cloud computing with technologies to provide the e Citizen with the overall benefits of mobile technologies.

- **To manipulate and use these pool of information (Big data)**
  The government can now extrapolate factor such as population growth and allocate the necessary resource. It can also predict the revenue from taxes just by how many companies are registering in the system. This pool of information could be used to benefit the state.

Big Data processing enables governments to make choices based on large-scale analysis. Goals include allowances for greater policy transparency, and identification of high social and economic value. Most broadly, data mining aids decision-making through the discovery of patterns in large data sets based on facts or observations. Data mining tools can process structured numeric data in traditional databases or extract relevance from semi-structured and unstructured data, such as text, graphics, images, and web data. Leveraging Big Data can enable breakthroughs in e-Government management, where, like the many industries using Big Data to identify opportunities for innovation, governments are able to act on the best available information.

Big Data processing is not simply waiting for automatic results; it is necessary to master the tools and skills to transform raw data into information, knowledge, and wisdom. Skills and techniques to be mastered include data warehouse integration, business intelligence, and data visualization, as well as business analysis and forecast modeling. In addition, organizations must develop appropriate work processes and policies, find talent for drawing sound conclusions to meet ever-changing citizen needs.

In summary, we must gather data from every part of the "Cloud" and extract knowledge from massive data collections to build core capabilities in the development of e-Government services.[9]

4.16 Feedback on the performance

People already do more than talk on their mobile devices. At the end of 2009, data transmission surpassed voice transmission on phones. According to data from the Pew Internet and American Life Project, people are using their cell phones to use more and more non-voice data applications. They take and share photos and video, play games, send and receive text and email messages, and access social networks and websites via mobile device.

The total number of text messages sent worldwide tripled between 2007 and 2010, from an estimated 1.8 trillion to a staggering 6.1 trillion. Breaking that figure down, 200,000 text messages are sent every second.

Consumer habits are changing too. Forrester research firm reported that people are increasingly more comfortable spending money, using price-comparison services and bar code scanners, and submitting consumer reviews on mobile devices. [10]

This itself gives us an idea how engraved mobile technologies have become part of out lifestyle. People could submit their insight and rate various govt departments according to their experiences. This will force the govt. to look into irregularities in the system, and encourage further improvement.

4.17. Results and Discussion

The aim of the solution is to demonstrate how e-government could be incorporated to provide a secure service without any paperwork involved. Issuing a passport is one of the most cumbersome process if done manually. It requires a lot of man hours, and extensive amount of paperwork, while it demands security and accuracy.

In terms of our results that we have achieved, we could say stick to the phase “Information is key” to offer an eGovernment service that is unique in terms of incorporating technologies and providing a hassle free service while preventing fraudulence or duplication.

The most useful aspect of the system is the ability to share information related to the issuance of the new document using various sources of authentication.

Furthermore the passport office could also enhance their data storing capacity by having a simple mechanism in place where the details of the people migrating can be fed into the system at the 'Point of Exit'.

Photographs could be uploaded directly from the mobile device, thus cutting down the need to have it taken from outside.

In a situation where the passport holder looses his document while traveling outside the country; a new passport could be issued with a few hours, since the paperwork and validation could be done within a few minutes as against the cumbersome manual validation.

In the event of applying for lost passport, it is usually necessary to submit a copy of the birth certificate. Instead of submitting this copy the user could simply enter the ID no of the birth certificate, and the passport office will retrieve it for you.

The citizens have the added advantage of tracking the progress of their request which is essentially a part of good governance. Therefore, this system also provides the ability for two way communication and better interaction.

Further down the line the success of any system depends on the security and the ability to protect it from vested interests.

For this purpose we have also discussed the preemptive measure that must be adapted in order to secure data and provide safety for it's users. Hence, we should implement different access layers.

A Code of Conduct must be established since not everyone should be allowed access to the information and the people that are allowed to access do not breach the trust placed in them to manipulate this data for any personal or commercial means. Personal with through background checks and clearance should have to be responsible for information handling.

Passwords and terms of login into the Cloud should be recorded in a log book.

Data encryption is also enabled and hence, hackers will be discouraged at any attempt to sabotage the privacy of the system.

As mentioned previously under the topic of Security we would implement a system where the client will be isolated using a Brokered Cloud Storage Access. We add a separate layer of access to by using a broker with full access to storage but no access to client. A proxy with with no access to storage but access to both client and broker.

The proxy will be the authoritative person responsible for dealing with client requests. And he/she will be responsible for requesting the information from the broker which has access to access to storage. This way we draw a line of isolation to enable privacy and direct contact with the client, thus enabling to separation of information.

4.18 Downside to effective implementation and success of the Cloud Computing System

Cost of Implementation

The need of a major investment by the government could discourage some states to implement the system. However, the long term benefits outweigh the initial outlay. Access to information is key in implementing govt. policies. Therefore, with the cut down of red-tape and the cost of new technological devices coming down low, the potential outlay could decrease over a period of time. Furthermore, this system could be a stepping stone for a fully automated government, thus making the phase eGovernment more feasible.

Internet penetration could be low.

It has to be understood that Internet is one of the key requirements of this system. However, due to the availability of Wi-Fi technology, even in cafes, and restaurants, individuals; no matter where they are traveling could access the service.

Doesn't appeal to the older segments due to lack of IT literacy.

People with low IT literacy could find the new system challenging. However, due to effective User Interface, we could ensure that atleast a part of this segment could be catered to in the near future, with incorporation of new technologies.

Not every smart-phone is always connected.

Smart phone users usually pay extra fees to service provider for Internet connectivity. Even though this might discourage some potential users, the convenience and the security of the system could be an attractive incentive.

5 Conclusion

The objective of the thesis is to provide an analysis for innovative solution to the public sector services, using a cloud computing model. Thus we have created a new instance of a solution that utilizes the power of Cloud Computing and mGovernment model, in approving and delivering a Passport to any individual with a mobile phone and access to the Internet, using the clients mobile device.

Therefore, we have:

- developed literature review of current state of online public services and cloud solutions.

- analyzed and designed a specific mobile electronic public service.

- made an evaluation of proposed solution.

We have successfully come up with a hassle free, on-demand, solution that satisfies the Governments need to deliver better services to the public no matter which part of the globe the request comes from, in a timely and a secure manner, and for citizens to obtain those services without wasting time.

At the same time we have made sure to follow the ITPOSMO guidelines and developed a Case Study based on the solution that will meet the most stringent standards of the industry.

According to the available options we have decided to use the hybrid option since it is most suitable for our layers. The first being the interaction between the public and the departments, and the second being the interactions between the departments.

As for our infrastructure requirements we could use SaaS methodology to build two layers of applications. The first being the layer required by the public to interact with the departments, and the second layer for the departments to interact with the platform, as this is the concept that would increase security in accordance with Brokered Cloud Storage Access.

The approach will be hybrid as the other methodologies do have limitations in terms of delegating necessary changes as and when required. These options were conceived based mostly on the security considerations, and the management of the overall system.

The example above is purely to convey the need for an e-government platform, and the benefits it could provide to both the citizens and the government in terms of using mobile technologies, and cloud computing to generate and store big data, while improving the coordinating capacity among various governmental institutions.

Technologies such as cloud computing can really improve governance and national security, while adding value to the service provided to the citizens.

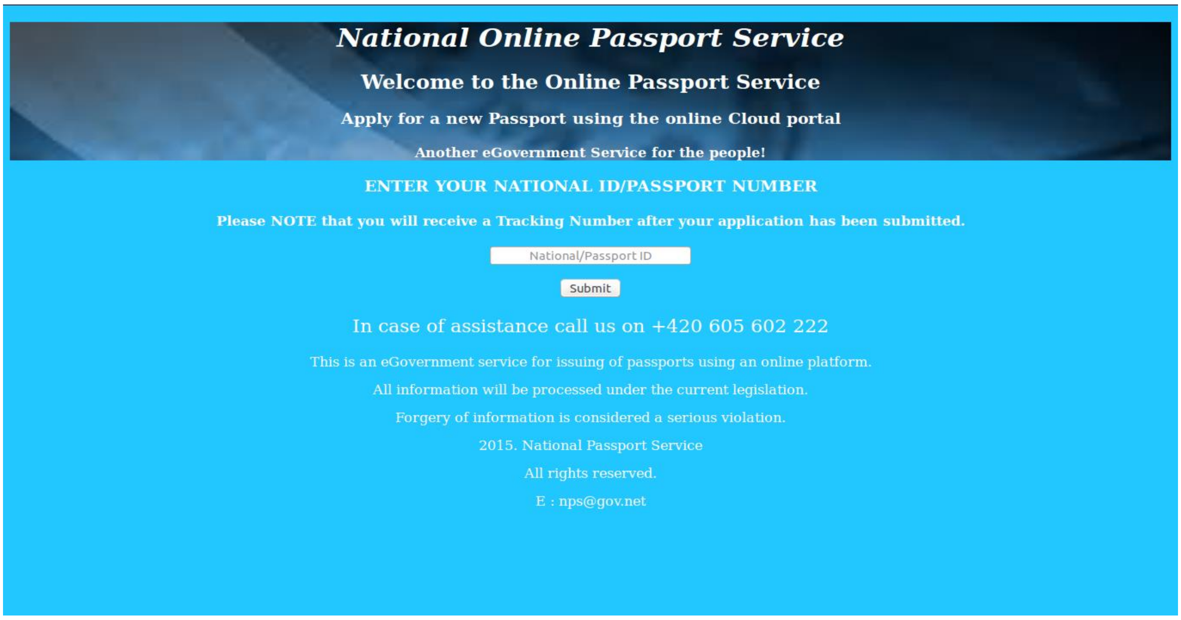
6 References

Bibliography

1. J. Satyanarayana, E-Government: The Science of the Possible, p. 100 PHI, 2004. ASIN: B00K7YFZ50
2. Ake Gronlund , Electronic Government: Design, Applications and Management, p. 388 IGI Global, 2001. ISBN: 1930708198, 9781930708198
3. Richard Hill, Laurie Hirsch, Peter Lake, Siavash Moshiri, Guide to Cloud Computing: Principles and Practice (Computer Communications and Networks), p. 278 Springer, 2012. ISBN: 1447146026, 978-1447146025
4. Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2015
5. Zaigham Mahmood, E-Government Implementation and Practice in Developing Countries (Advances in Electronic Government, Digital Divide, and Regio), IGI Global, 2013, p. 348. ISBN: 1466640900, 9781466640900
6. Heeks, R., Implementing and Managing E Government: An International Text. Sage Publications, 2006, p. 293. ISBN: 9780761967927
7. Peter Wood, How to tackle big data from a security point of view, http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view, Accessed on 29-02-2015
8. Mararet Rouse, Intrusion Detection, 2007, http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection, Accessed on 27-02-2015
9: Zhao Qing, Three Development Trends in e-Government: Cloud, Collaboration, and Big Data, http://www.huawei.com/enapp/2679/hw-275536.htm, Accessed on 07-02-2015
10: , Discover: The Case for Citizen Centric Mobile Gov, http://www.gsa.gov/portal/content/288913, Accessed on 09-03-2015

6 Supplements

Proposed model of the Welcome page



National Online Passport Service

Welcome to the Online Passport Service

Apply for a new Passport using the online Cloud portal

Another eGovernment Service for the people!

ENTER YOUR NATIONAL ID/PASSPORT NUMBER

Please NOTE that you will receive a Tracking Number after your application has been submitted.

In case of assistance call us on +420 605 602 222

This is an eGovernment service for issuing of passports using an online platform.

All information will be processed under the current legislation.

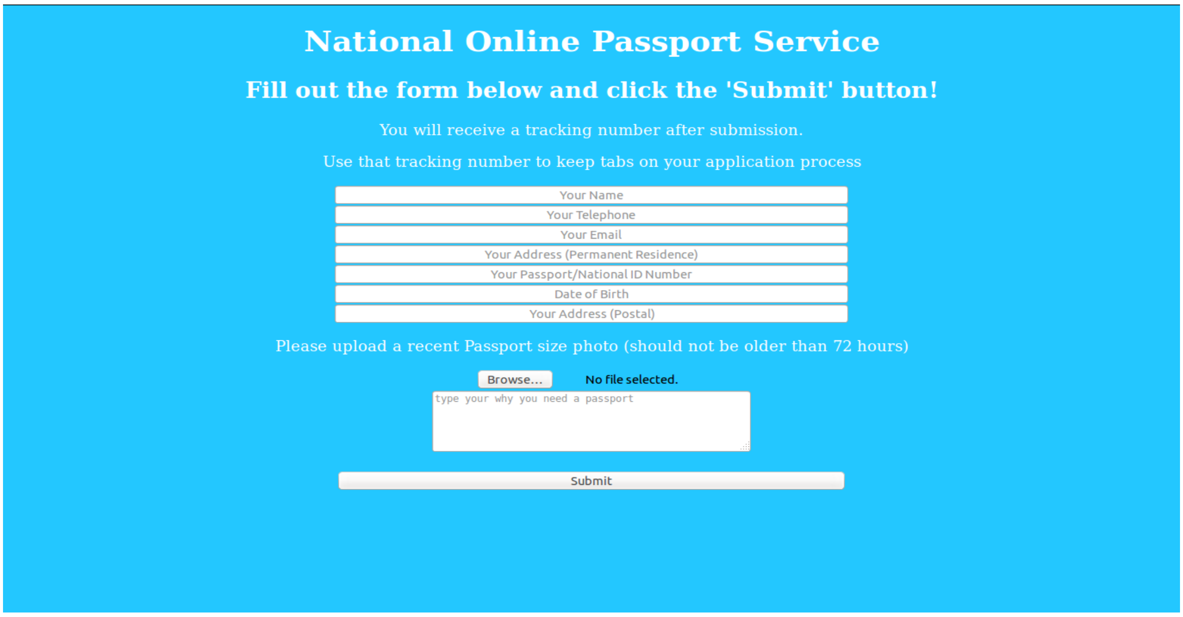
Forgery of information is considered a serious violation.

2015. National Passport Service

All rights reserved.

E : nps@gov.net

The form that should be filled by the Client.



National Online Passport Service

Fill out the form below and click the 'Submit' button!

You will receive a tracking number after submission.

Use that tracking number to keep tabs on your application process

Your Name
Your Telephone
Your Email
Your Address (Permanent Residence)
Your Passport/National ID Number
Date of Birth
Your Address (Postal)

Please upload a recent Passport size photo (should not be older than 72 hours)

Browse...
No file selected.
type your why you need a passport
Submit