Future Computing and Informatics Journal

Volume 3
Issue 2 *Vol 3,Issue 2,2018*

Article 13

2018

A proposed hybrid model for adopting cloud computing in e-government

Kh. E. Ali
Department of Information Systems, Faculty of Computers and Information, Cairo University, Cairo, Egypt, k.ali@pg.cu.edu.eg

Sh. A. Mazen
Department of Information Systems, Faculty of Computers and Information, Cairo University, Cairo, Egypt, s.mazen@fci-cu.edu.eg

E. E. Hassanein
Department of Information Systems, Faculty of Computers and Information, Cairo University, Cairo, Egypt, e.ezat@fci-cu.edu.eg

Available online at www.sciencedirect.com

ScienceDirect

Future Computing and Informatics Journal 3 (2018) 286–295
http://www.journals.elsevier.com/future-computing-and-informatics-journal/

A proposed hybrid model for adopting cloud computing in e-government

Kh. E. Ali*, Sh. A. Mazen, E.E. Hassanein

Department of Information Systems, Faculty of Computers and Information, Cairo University, Cairo, Egypt

Received 17 August 2017; revised 16 June 2018; accepted 13 September 2018
Available online 19 September 2018

Abstract

Many developing countries are now experiencing revolution in e-government to deliver fluent and simple services for their citizens. However, governmental sectors face many challenges in using its e-governments' services and its infrastructure, improving current services or developing new services; as data and applications increasingly inflating, IT budget costs, software licensing and support and difficulties in migration, integration and management for software and hardware. These challenges may lead to failure of e-governments' projects. Therefore, there is a need for a solution to overcome these challenges. Cloud Computing plays a vital role to solve these problems. This paper demonstrates e-government's obstacles and cloud computing features. Also, it proposes an abstract hybrid model for adapting cloud computing in e-government that overcomes the e-government's challenges. This hybrid proposed model identifies three different patterns of cloud computing which are Local Governmental Cloud "LGC", Regional Governmental Cloud "RGC" and Wide Governmental Cloud "WGC". The proposed model determines how the entity connects to each of three clouds and what the relation between them is. In addition, readiness assessment of the services need to migrate into cloud. Finally, a set of recommended cloud aspects and their values for each of three clouds are suggested that ensure implementation of the sorted services.

Keywords: Cloud computing models; E-government; E-government's challenges; Governmental cloud

1. Introduction

The last two decades have witnessed the wide diffusion of e-government adoption in many countries because it has many benefits for citizens and governments. For citizens, it can manage data, enhance public service delivery and expand communication channels. For governments, it will increase productivity, grow business economy, share global knowledge and have automated business processes and communications. Although all these benefits for e-government, there are many of drawbacks for it.

Since 2009, researchers have been investigating cloud computing in the context of e-government. Literature on this context shows there are many of obstacles prevent e-government's project to success, modernize and add new services and how cloud computing can overcome these obstacles.

The rest of this paper is organized as introduction in previous section. The following section will discuss the basics of cloud computing and some related work for adopting cloud computing in e-government. Thirdly, the role of cloud computing in e-government will be discussed. The next part is the proposed hybrid model for adopting cloud computing in e-government. Finally, we put our conclusion and future work.

2. Literature review

There is no research defines cloud computing without mention the common definition for National Institute of Standards and Technology (NIST) which, defines cloud computing as Khajeh-Hosseini et al. (2012) and Badger et al., (2011) "the a model for enabling ubiquitous, convenient, on-

* Corresponding author.
E-mail addresses: k.ali@pg.cu.edu.eg (Kh.E. Ali), s.mazen@fci-cu.edu.eg (Sh.A. Mazen), e.ezat@fci-cu.edu.eg (E.E. Hassanein).
Peer review under responsibility of Faculty of Computers and Information Technology, Future University in Egypt.

https://doi.org/10.1016/j.fcij.2018.09.001

demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" as in Refs. [3] and [21].

There are many of delivery models of cloud computing as SaaS, IaaS, DaaS, PaaS, and NaaS but many researchers listed SaaS, PaaS and IaaS as the most important and the most widespread [1,4,6,11–13].

The NIST, many of researchers defines four deployment models according to [1,2,4–6,21]:

- Public Cloud: Public cloud services are characterized as being available to clients from a third party service provider via the Internet. A public cloud does not mean that a user's data is publically visible or free to use; public cloud vendors typically provide an access control mechanism for their users.
- Private Cloud: In a private cloud, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.
- Community Cloud: A community cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.
- Hybrid Cloud: A hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

After reviewing some concepts of cloud computing, we will investigate some models for adopting cloud computing in e-government environment.

- Ahmad and Hasibuan, 2012 developed initial architecture for implementing e-government based on cloud computing in Indonesia, which consists of six layers: infrastructure, virtualization, management, service, access and user layers [13]. This architecture allows for greater information, resource sharing and promote more standardization in the government's resources. In addition, for deployment model, the hybrid cloud approach is recommended based on the characteristics of e-government relationships in Indonesia. They also get findings that implementing cloud based e-government architecture can significantly reduce costs of ICT investment.
- Hana, (2013) developed an abstract hybrid model to adapt national e-government in Egypt to cloud computing in order to reduce the cloud computing risks associated with security, privacy, reliability, performance and legal issues without ignoring any of the current concepts of cloud [38]. This proposed model consists of three types of cloud computing which are Intra-Cloud computing (IACC), Extra-Cloud computing (EXCC) and Inter-Cloud computing (IECC). The proposed model enables each of three clouds set a number of constraints and restriction yet permits maximum integration, communication and collaboration among them.
- Karokola, (2012) proposed a framework for securing e-government services. It was developed in response to the security problem in e-government services that is caused by many reasons including the lack of security services in eGMMs [39]. The proposed framework addresses both the quantity of offered e-government services and the quality of security services by aligning strategic objectives between e-government services and security services. Therefore; it will mitigate the current and emerging security risks and threats posed to e-government services; hence enhances confidentiality, integrity and availability of critical information assets being stored, processed, and transmitted within and between e-government domains.
- Singh and Chandel, (2014) proposed a cloud framework for Indian government through the integration of the functioning of various departments among the different states under the Indian National e-Governance Plan [17]. This integration between the separated data centers for each state connected by State Wide Area Networks (SWAN). These different networks can be integrated together logically over the cloud so that the concerned authorities may be provided instant access to the desired information without any delays and barriers to communication across the states. This connection ensures interoperability functionality among different states and it reduces the operating costs, provide greater reliability, transparency and sustainability while using latest technologies.
- Kumar et al., [40] proposed a cost effective framework for e-governance in India by using Free and Open Source Software (FOSS) for development and deployment of e-governance applications, virtualization and consolidation techniques for management of e-services and cloud computing for enhancing the accessibility of services among citizens including rural masses [19]. This will lead towards reduction in total cost associated with both hardware as well as software. Therefore it reduces the financial burden abide by the state and central governments.

3. Applicability adopting cloud computing in e-government

However, based on our investigation in related literature, there are many inhibitors prevent utilizing e-government; we decompose into technical and nontechnical inhibitors:

Technical inhibitors as: Duplication of applications and data, insufficient exchange and logging details of client's data,

difficulties in migration, integration and management for software and hardware, poor capabilities with disaster recovery, auditing and logging, fragmentation of resources and low asset utilization, software licensing and support, traditional infrastructure cannot scale, security and privacy, and poor performance with rapidly changing in the system requirements.

Non-technical inhibitors as: Traditional infrastructure incurs more costs during modernization and modifications of infrastructure and software, physical security, skills, culture and the fear factor of employees and citizens, weak management and coordination between departments, power usage, air-conditioning and electronic waste could create biohazards and lack of accountability and management policies.

All these inefficiencies negatively affect the e-government's ability to serve the government's organizations. Cloud computing has the potential to play a major part in addressing these inefficiencies and improving government service delivery.

After study and analyzing the literature, we can summarize the benefits of adopting cloud computing in different aspects of e-government as in Table 1.

4. Obstacles in cloud e-government

Although many previous benefits are found in utilizing cloud computing in e-government environment, there are still many issues and challenges that need to be addressed. When third parties are treating with and processing sensitive data especially in government sector, it is obvious that concerns related to trust would be there in the mind of e-government's stakeholders. Trust is an act of firm belief in reliability, confidence, the capabilities and skills of others that you think you can reasonably rely on them to care for your valuable assets [26]. Trust is playing an important role in the success or failure of e-government system that citizens should have confidence in it. Some of the challenges when adopting cloud computing in e-government are discussed below:

4.1. Lack of data control

The first and obvious issue is the government losing control and ownership of data. When we have less control over our assets then we trust the system less [41]. Since data are stored in the cloud, data will be located at third party data centers where we have less control over data and the cloud computing providers have complete access to sensitive data.

4.2. Security and privacy

In Cloud Computing data and information is not stored and processed locally at the enterprise premises and the data are accessed through an open network. In fact third parties are responsible for storing and processing of data at their own sites [26]. In a situation like that individuals are concerned about the privacy of their personal data and information. When third parties are processing important data stored at remote machines at various locations it is obvious people would be worried about the privacy of their personal data because it is a human right to secure their private and sensitive information.

4.3. System failure

Another potential issue is system failure, there are some public services which should be available to citizens 24/7 but these services are unavailable to the citizens at some times [35]. Also the performance issue, especially for data intensive computation as client machines are geographically distanced, which could be a thousand miles away from the cloud. Finally, internet speed will definitely affect the performance. The possibility of data transfer bottlenecks as the intensity of data processing and transfer as well as the number of users accessing the data increase may complicate the performance and costs as data transfer consumes communication bandwidth.

4.4. Access authorization

It is the responsibility of the cloud service provider to keep the management interface secure from the unauthorized access because the management functionality should be accessible by few authorized administrators. Access authorization is required in order to give access to authentic users through claim base access control [29].

4.5. Data leakage

Data leakage can be also the main reason of discouragement for the government to use cloud based e-government system because it affects the trust of citizens and governmental organization in cloud based e-government system [41]. E-government system contains sensitive data and information about users and businesses therefore security of the sensitive and secured data is important.

5. Proposed hybrid governmental cloud computing model

5.1. Gathering the services/applications required to migrate into cloud

Firstly, we need to make many meetings with decision makers in order to identify all departments and applications will be included in the new domain and to identify the project boundaries. In addition, collecting the services required to migrate into cloud.

5.2. Classification the services according to some domains (functionality and properties)

Before identifying which the services will be migrated to cloud and which will be delayed, we need to classify these services into number of main categories: Static services, dynamic services, costly services, cheap services, secret services, and fewer secret services.

Table 1
Traditional e-government and cloud computing role.

No	Aspects	Traditional e-government	Cloud computing role
1	Availability and Accessibility [7–10]	Traditional IT abilities are limited to make services online all time. The insufficiency of electronic service is affecting the trust of the citizens in online services.	Applications and information are hosted online 24/7 with just one PC and Internet connectivity therefore it has high availability and citizens can use them at anytime and from anywhere, all these tasks are responsibility of system provider.
2	Fragmentation of resources and insufficient exchange of client's data [13–16]	Many different platforms for many e-services and places, in addition many of servers and resources in different countries. How can we connect all these different infrastructures and transform data between them? It will be difficult and non-accessible by the citizens as well.	Cloud computing helps the government in establishing a common platform for all its applications, one that is easily and universal accessible by the citizens as well. By adopting cloud computing, government agencies can create a central data pool of shared resources, software and infrastructure.
3	Performance and data scalability L. [17,18,20,21]	The general environment of government has an important feature is continuous changing in the rules and requirements, this required high capabilities of information technology weather manpower, resources or software for responding these changes and to deal with large data over the years	Cloud has scaling capabilities and can be used for this type of applications. Its database becomes large without disruption to its performance. Cloud users are able to scale back the amount of storage space needed, or raise it according to the pattern of growth. With an on-demand integration of cloud services, the consumers can quickly and easily increase or decrease connections, transactions, or the number of services in their integration community, and then scale up when resources requirement increases.
4	Disaster recovery [20,22]	Multiple installations in geographically separated locations with complete backup and recovery solutions must exist. This could create huge problems with there is no any disaster recovery strategy for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure in case of a damage. The disasters as floods and fires could cause loose not only the applications and data, but also make services unavailable. In addition, traditional disaster recovery applications are very slow to restore data, non-simple, complex and non-effective, so disaster recovery costs and recovery time are long, so government agencies are therefore worried about the loss of data and creating recovery backups.	In cloud computing, the techniques can identify and prioritize the applications, services and data, and determine for each one the amount of downtime that is acceptable before there is a significant business impact. IT profissionals professionals in governments are responisibleresponsible for storing a backup of the data and files using the cloud cababilitiescapabilities as a backup for any disaster recovery, daily and they should store it in a different location (off-site). The disaster recovery costs and recovery time are reduced; therefore, in the cloud, the disaster recovery apps support more options than traditional disaster recovery programs for organizations to restore data very quickly and effectively. The cloud offers tools and technologies that make disaster recovery simple and easy. Cloud offers distributed and virtualized system to implement data center policies with respect to security and application deployment, so IT profissionals are therefore not worried about the loss of any information or files.
5	IT standards, systems' integration and legacy' software [23–25]	There are many external entities have internal systems need to integrate, communicate, collaborate and share data automatically with each other; government cannot do this integration because difference in infrastructure, platforms and database.	Cloud computing technologies cooperate and interconnect with legacy systems and sometimes with each other, so an organization that is ussingusing an application on an internal cloud should be able to migrate to another cloud infrastructure without having to rewrite the application. The cloud computing is working to develop standards and interfaces for the interoperation of various types of software that support any integration.
6	Redundancy of data and applications [26–28]	Many of government agents have access on the same application and centralized database. Traditionally, there are many of applications take more time, effort, resources and budget not for development only, also for management these e-services. This happens for all the instances of these applications if we want to translate it into English and French.	Cloud technologies reduce the time and efforts to develope or deploy a new application instance because it offers more efficient opptionsoptions to create an instance of application for producing a new feature without any redendencyredundancy.

(*continued on next page*)

Table 1 (*continued*)

No	Aspects	Traditional e-government	Cloud computing role
7	Auditing and logging [25,27–29]	There are millions of transactions every day for hundreds of customers, government need to traceability system responsible for moderating any changes of information contents. Process audits and access right have to be done periodically for analyzing huge volumes of data and detecting any fraud to ensure the security of the system.	Cloud computing provide adequate logging and auditing features for all customers and transactions to ensure privacy and security. An external audit can be beneficial for strengthening the trust with the customer especially in government sectors. Traceability for any changes in data is necessary in e-government services. This help building defense mechanisms for suportingsupporting and increasing the security.
8	Obsolete technologies and migration to new technologies [24,30–32]	There are many numbers of computing resources (servers and computers) are consumed with time without any using its full capacity. In addition, there is no any software management (License, Effort and time), backup or maintenance strategy for these resources.	Cloud architectures provide efficient use of computing resources because it can estimate the workload of the servers and the applications so it can handle and manage the resources and thus have an incentive to consume only what we need.
9	Reporting and intelligently [33,34]	Traditional IT's abilities are limited to manage the e-services and generate some of reports by these reports we can identify the servers performance. This is necessary to make better resource utilization.	Cloud computing can provide its business by intelligence software, which generates custom reports required for executive, management and user levels by these reports the government agencies can identify the servers performance. The intelligence software gathers more data to meet the key performance indicators about data center, the peak load, consumption level and use of energy along with time. Applications can extract large amounts of reliable data to make the best decisions to providprovide better services and low costs.
10	Cost and Budget [5,34–36]	The global economic crisis, especially in developing countries, affect most fields as industrial and commercial business then sure, it will affect information technology field, so it is not easy to allocate big budget for many IT centers in government sector. Therefore, we need to get maximum numbers of e-services in minimum cost.	Cloud computing architicturesarchitectures reduce and eliminate capital expenditures and reduce ongoing operating expenses by: Fully utilized hardware and software license: optimizing the hardware needs of its data centers and software licenses, which mean lower costs for government sector. Lower power costs: Better hardware utilization means more efficient power use therefore cloud-computing uses less electricity. Lower people costs: The staffing budget is usually the biggest item in the budget; Good IT people are expensive; their salaries, benefits, and other employment costs usually outweigh the costs of hardware and software.
11	Green Computing [13,35,36]	The power usage, air-conditioning and electronic waste could create biohazards, so today more governments emphasize on the amount of pollution can be created in the data centers.	This could be one of the reasons for moving to cloud architecture in governance. Instead of duplicating these facilities, with cloud, one can offer centralized infrastructure that can be efficiently used to minimize pollution is resulted of CO2
12	Lack of accountability and management policies [5,37,39,40]	At the government's agencies, there is the belief IT man is responsible for anything technical in the organization without distribution for any roles or responsibilities, on the other side the employee can repair or support any failure in the software or hardware he use. Therefore, some of end users may be asked to finish tasks are not their specialty, this may lead to many of resources, efforts and times are wasted. RRR. In addition, there are a large number of end users need huge amounts of changes and modifications in the systems and resources but IT team is wasted in these tasks. All these work forces are unorganized and distributed in randomly way.	The onus of any technical problem as upgrading technology is on the service provider in this delivery model who ensures access to the most up-to-date solutions, secured data, systems availability in 24x7, and system's support and maintenance. Apart from reducing the workload, this reduces the need for IT staff and allows the government agencies to focus on their core areas of work.

There are many dependencies and overlaps between the categories, such as the relations between the static services and cheap services. In addition, there are relationships between the categories of dynamic services and costly services. Generally with perspective of IT professionals in government and their possibilities and security

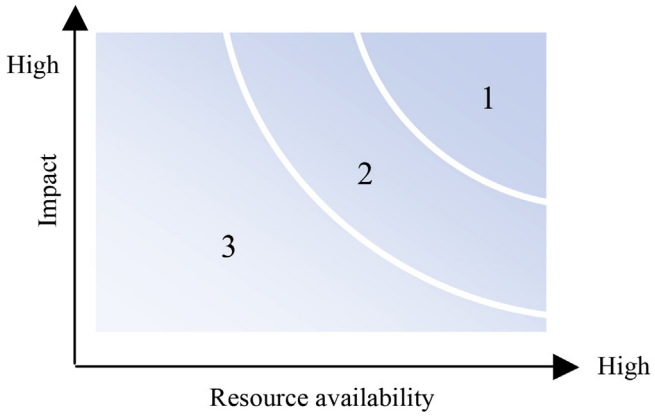

Fig. 1. Prioritizing services for cloud migration.

considerations, they can determine which service in which category.

5.3. Services readiness assessment

Governmental entity moves its e-services gradually from traditional e-government into cloud technology. Therefore, we need to assess the readiness degree of all services required to move into cloud. In this stage, we declare the categories of services move to cloud firstly, which will be delayed some time and which will not move and need to some substantial changes in the business and workflow, according to this proposed model. Which identifying two dimensions impact and resources availability for each service as shown below in Fig. 1, services with relatively high impact and high resource availability are strong candidates to move to the cloud first (area 1) then area 2 and finally the services in area 3;

In impact dimension, it captures the aspects of each service that has benefits for the organization in the three levels (citizens, society and government).

- For citizens: Saving time, money and effort, improving the services to people in the form of faster and easier, building trust between citizens and governments, managing data and ease of finding information, improvements in service delivery quality and expand communication channels, increase the transparency of decision-making processes by making information accessible for citizens and they are better equipped to make better decisions.
- For society: Increasing the skills, awareness and culture of the community, enhancement the cooperation and joining between people in the society, promoting social inclusion, particularly of disadvantaged and vulnerable groups, sharing the global knowledge, information and ideas, can help stakeholders boost use of an educational, experiments, researches or training program, creating new business and work opportunities, better health and education and community goes green.
- For government: Cost saving to agencies in the form of simpler and speedier transactions, helping reduce corruption, increases openness and trust in government, and thus contributes to help in the reform economic and political program, increasing effectiveness by productivity and grow economy, improving efficiency by making paperwork is so simple, making daily processing tasks are easier and facilitation public administration operations, web-based applications can generate savings on efforts and time, providing data collection and transmission and provision of information and communication with customers, enhancing accountability; ICT helps to increase information available for people, make each one, each department and each management judging himself and full support for IT staff, concentration in the technical works only, more training and experience and saving their time and effort.

Resources availability dimension: it captures the ability of organization to accept this service to move into cloud and classified to two categories.

- Determinants before and during migration: Technology (HW and SW), human resources (experience), safety/cause problems, security, availability, performance, reliability, scalability and portability.
- Capabilities after migration: organization/employees, laws, policies and regulations readiness, market readiness, technology readiness (Data is safe, authenticated, authorized, complete, accurate and compatibility) and customer satisfaction.

5.4. Governmental cloud implementation

As, we proposes a conceptual hybrid model for adopting cloud computing in e-government consists of three computing cloud; Local-Cloud computing, Regional-Cloud computing and Wide-Cloud computing. The three cloud models are analogs to the terms LAN (Local Area Network), MAN (Metropolitan Area Network) and WAN (Wide Area Network) which are three types of the network designed to operate over the area they cover in their functionality, operation and management. Each model allows devices to connect via any connector, integrate, communicate and collaborate applications and data with different devices according to specifications, constraints and restrictions of each model.

- Local Governmental Cloud (LGC)

LGC is a classified cloud in which data and processes are managed within the organization or entity without the restrictions of network bandwidth, security exposures and legal requirements because the users of this type are employees are only located in the organization as shown in Fig. 3. In addition, LGC provides three basic delivery models of cloud computing services SaaS, PaaS and IaaS, therefore it offers the provider and the user greater control of the cloud infrastructure, applications, improving security and resiliency because user access and the networks used are restricted and designated. The links network devices in such a way that connect

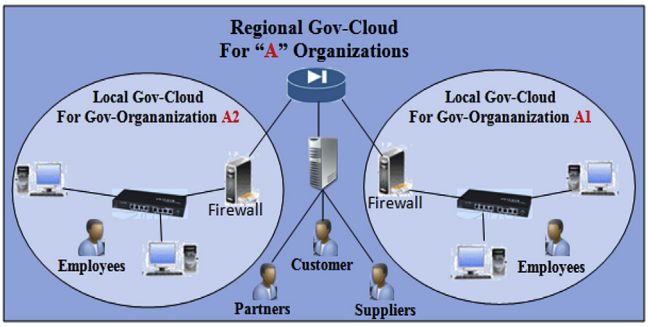

Fig. 2. LGC and RGC for national region A.

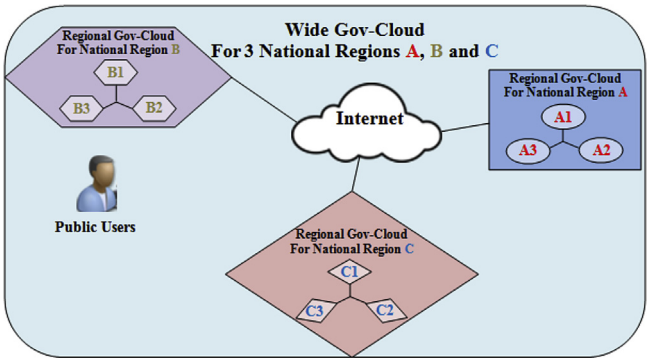

Fig. 3. WGC for national three regions A, B and C.

workstations can share and transmit data, tools and programs at a very fast rate as the number of computers linked are limited. LGC covers smaller geographical area and are privately owned by entity or e-government organization which is easy to design and maintain.

- Regional Governmental Cloud (RGC)

RGC is a combination cloud covers a larger geographical area than that of a LGC and smaller area as compared to WGC so the data transfer rate of RGC is moderate therefore the users of this cloud are external entities as customers, partners and suppliers as shown in Fig. 2. It connects two or more entities that reside in the same or different cities; therefore it is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. It may serve a provider to another entity so it's hard and costly to design and maintain and it may or may not be owned by a single organization. Finally, RGC provides three basic delivery models of cloud computing services SaaS, PaaS and IaaS.

- Wide Governmental Cloud (WGC)

WGC is a universal cloud allows all public users to utilize its services. It extends over a large geographical area. Its services are characterized as being available to clients from a third party service provider via the internet as shown in Fig. 3. WGC does not mean that a user's data is publically visible or free to use; public cloud vendors typically provide an access control mechanism for their users. Due to long distance transmission, the noise and error tend to be more in it. Propagation delay is one of the biggest problems faced here. Finally, WGC provides three basic delivery models of cloud computing services SaaS, PaaS and IaaS. WGC consists of three layers:

1) Front Layer: This layer is in the foreground of WGC, which is responsible for managing the users' registration, requirements, authentication, security, modification, processing, connecting with other layers and finally response the user. Front Layer consists of two types of users; entity (may be a provider or customer) and public user.
2) Services Layer: This layer is responsible for provisioning, managing and automation all services users need. It consists of three systems (Development, SaaS and GaaS); in development system, user can use available tools and platforms to produce or customize any service he need, Data mart and Knowledge management. In SaaS system, user can use any available public service as email, change management, ERP, virtualization management, Digital signature, Workflow, Web applications or any on the shelf apps. In GaaS system, user can use the governmental service as voting, insurance, traffic or any other governmental system.
3) Physical Layer: This layer is base layer which represents all physical elements/hardware users need on cloud service, including servers hosting, storage, network, and workstations.

5.5. Governmental cloud allocations

This section determines recommended important aspects in cloud computing implementation. It identifies the most appropriate proposed governmental cloud (LGC, RGC or WGC) for each e-service has a highly priority in (area 1). Those practices are categorized into technical aspects, organizational aspects and environmental aspects. Each category contains a set of specifications with their recommended values.

5.5.1. Technical aspects

This category includes some specifications concentrate on technical view of services and their values for all three types of governmental clouds as in Table 2: Services availability; it specifies the available boundaries of the end user can access the service. Fragmentation of resources; it refers to the resources places required to deploy the service. Security; it indicates the constrains and the techniques required to secure the service. Data scalability; it refers to ability of scaling in and out of the data used in the service. Services customization; it refers to the changes required in the service to be compatible with business requirements. Disaster recovery; It is the manner and the cost of the dealing with service in case of catastrophe. Applications Integration; it refers to how the service can integrate with legacy systems and other applications.

Table 2
Technical aspects and their values for proposed model.

Seq	Aspects	LGC value	RGC value	WGC value
1	Services availability	Inside organization only	Identified by organization or community	Available any where
2	Fragmentation of resources	Only in the organization	in the organization or fragmented in the community	Fragmented in many places
3	Security	High	High	Medium
4	Data scalability	Easy to scale	Medium in scalability	Difficult in scalability because lock provider who refuse continues changes in requirements
5	Services customization	Low in size and Excellent features	Moderate	High in size and difficult to customize
6	Disaster recovery	Easy and cheap	Moderate according to size of community	Complex and expensive
7	Applications Integration	Easy and simple in integration	Moderate	Complex
8	Configurable cloud requirements S.W/H.W	Limited	Moderate	High
9	Auditing and logging	Perfect	Natural	Difficult
10	Data processes	Most operational and less aggregation	Operational and aggregation	All operations
11	Number of transactions	Small transactions	Medium according to size of community	Many transactions
12	Services types	More specific apps for specific entity	General apps for specific community	More general apps for any entity
13	Data physical Location/Manipulation /Transfer/Administration	In house	In house or off house	Off house
14	Data transmission errors and noise	Low	Moderate	High

Configurable cloud requirements S.W/H.W; it specifies the requirements of setting up and deploying the services in the cloud. Auditing and logging; it collects and manages the log history of users' transactions. Data processes; it refers to the type of operations can be made on the data. Number of transactions; it indicates the number of transactions that user do to finalize that service. Services types; it refers to the type of services deployed in each cloud which depends on the using size of that service. Data physical Location/Manipulation/ Transfer/Administration; it refers to the physical location in where the service can be manipulated and managed by the administrator. Data transmission errors and noise; It indicates to delay time and error rate during data transmission to perform the service.

Table 3
Organizational aspects and their values for proposed model.

Seq	Aspects	LGC value	RGC value	WGC value
1	Accountability and administration	The entity only	The organization, government provider or trusted third party provider	Third party provider
2	Intelligently and decision support	Fully support and help	Fully support and help	Very much support and help
3	User access rights	Easy	Moderate	Difficult
4	Cloud Administration	Perfect in control and management	Medium in control and management	Complex and difficult to manage the resources
5	User confidence	Trusted	Trusted	Trusted and un-trusted
6	Accessibility by users	Users in house	Users In house and shared community only	Any one
7	Cloud service owner	Entity	Entity or trusted third-part provider	Trusted third-part provider

Table 4
Environmental aspects and their values for proposed model.

Seq	Aspects	LGC value	RGC value	WGC value
1	Green Computing	Low	widely	The best in green computing
2	Governing law and regulations	National	National or international	International
3	Partnership with others	No give or Take	May give or take with trusted entities	Yes give or Take
4	Area covered	Very small Location	Moderate (Group of buildings)	Spread world wide
5	Congestion	Less congestion	Moderate	More congestion

5.5.2. Organizational aspects

This category includes some specifications concentrate on organizational view of services and their values for all three types of governmental clouds as in Table 3: Accountability and administration; it refers to the responsible for deploying, managing, technical supporting and availability of the service. Intelligently and decision support; it identifies the extent of utilization for that service for the entity. User access rights; it indicates to the ability of administrator to identify transaction's time, transaction's user and transaction's activities. Cloud Administration; it refers to the management manner and the control level of the resources in each type of cloud. User confidence; it specifies the user's types who the entity trust in them. Accessibility by users; it identifies the boundaries of end user can access the applications. Cloud service owner; it is the entity that legally owns the cloud within which the cloud service resides.

5.5.3. Environmental aspects

This category includes some specifications concentrate on environmental view of services and their values for all three types of governmental clouds as in Table 4: Green Computing; it indicates to which type of cloud is responsible and eco-friendly use of computers and their resources in a way that reduces their environmental impact. Governing law and regulations; it identifies the laws and regulations control and manage contracting process and how to litigate in case of disputation. Partnership with others; it identifies the ability of sharing the service with other entities. Area covered; it identifies the physical location and its boundaries that each cloud covers. Congestion; it indicates the number and size of services and resources in each cloud.

For each e-service, the decision makers give a weight value for each aspect and identify the proposed governmental cloud according to Tables 2–4, then sum the values for each cloud type. Finally, the maximum value in the summation, it is the location of that e-service.

6. Conclusion and future work

This paper reviewed some of e-government and cloud computing specifications, discussed some obstacles may lead to failure of e-governments' projects and how can cloud computing overcome these difficulties. Also, it proposed an abstract hybrid model to adapt cloud computing in e-government; which identifies and classifies e-services according to specific domains. In addition, this proposed model identified three types of governmental cloud computing; Local Governmental Cloud “LGC”, Regional Governmental Cloud “RGC” and Wide Governmental Cloud “WGC”. It can determine e-services readiness; which e-service is ready now to migrate into cloud and which will be delayed sometimes, therefore it prioritizes the e-services to be migrated into proposed governmental clouds. Finally, it recommended a set of cloud aspects and their values for each of three proposed governmental clouds. This proposed conceptual model for cloud computing adoption in e-government context paved the way for developing practical framework helps prioritizing the e-services need to move into government cloud and identifying its cloud deployment model. When the organization moves from state to another, it needs to measure the impact of adopting cloud on the organization and compare between two states. In addition, putting alternative plans and moving back from cloud platform to a non-cloud platform if it did not meet the requirements of adoption process. What could be the reasons behind such a move and how will it impact the platform strategy of future?

Last but not the least, is it likely in any scenario for an organization to take an interest in two phases (before and during) of the cloud computing adoption. Therefore, the findings of this paper consider a good introduction for proposing a framework assist the organization in managing, monitoring and following up its performance after adoption the cloud computing.

References

[1] Singh H, A. P. S. N. Campus. Technology transfer model to migrate e-governance to cloud computing. IJATER (Int J Adv Technol Eng Res) 2012;2(4):52–7.
[2] Conway G, Curry E. Managing cloud computing-A life cycle approach. CLOSER; 2012. p. 198–207.
[3] Khajeh-Hosseini A, Greenwood D, Smith JW, Sommerville I. The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. Software Pract Exp 2012;42(4):447–65.
[4] Shimba F. Cloud computing:strategies for cloud computing adoption [Masters dissertation]. Dublin: Dublin Institute of Technology; 2010.
[5] Tweneboah-Koduah S, Endicott-Popovsky B, Tsetse A. Barriers to government cloud adoption: the ghanaian perspective. Int J Manag Inf Technol 2014;6(3):1.
[6] Wyld DC. Moving to the cloud: an introduction to cloud computing in government. IBM Center for the Business of Government; 2009.
[7] Gronlund A, Horan TA. Introducing e-GOV: history, definitions, and issues. Commun Assoc Inf Syst 2005;15(1):713–29.
[8] Luna-Reyes LF, Pardo TA, Gil-Garcia JR, Navarrete C, Zhang J, Mellouli S. Digital government in North America: a comparative analysis of policy and program priorities in Canada, Mexico, and the United States. In: Comparative e-government; 2010. p. 139–60. https://doi.org/10.1007/978-1-4419-6536-3_7.
[9] Nations U. United Nations e-government survey 2014: E-government for the future we want. United Nations Department of Economic and Social Affairs; 2014.
[10] Li G, Zhang QP, Wang W, Feng ZQ. Analysis on influence factors of implementing e-government public cloud. Appl Mech Mater 2013;411:2157–60.
[11] Nasr AO, Galal-Edeen GH. Proposed development model of e-government to appropriate cloud computing. Int J Rev Comput 2012;9(7):1–7.
[12] Rastogi A. A model based approach to implement cloud computing in e-governance. Int J Comput Appl 2010;9(7):15–8.
[13] Ahmad M, Hasibuan ZA. Government services integration based on cloud technology. In: Proceedings of the 14th international conference on information integration and web-based applications & services. ACM; 2012. p. 303–6.
[14] Taher Y, Haque R, Nquyen DK, Van den Heuvel WJ. Designing and delivering public services on the cloud. In: International conference on cloud computing and services science; 2011.
[15] Trivedi H. Cloud computing adoption model for governments and large enterprises [Doctoral dissertation]. Massachusetts Institute of Technology; 2013.
[16] Lee J. 10 year retrospect on stage models of e-government: a qualitative meta-synthesis. Govern Inf Q 2010;27:220–30.

[17] Singh VJ, Chandel A. Evolving e-governance through cloud computing based environment. Int J Adv Res Comput Commun Eng 2014;3(4):6188–91.
[18] Maluleka SM, Ruxwana N. A framework for cloud computing adoption in South African government: a case of department of social development. In: Proceedings of international conference on business management & IS, vol. 2; 2013. No. 1.
[19] Veljanovska K, Zdravevska V. E-government based on cloud computing. J Emerg Trends Comput Inf Sci 2013;4:377–81.
[20] Mohammed F, Ibrahim O. Refining e-government readiness index by cloud computing. Jurnal Teknologi 2013;65(1).
[21] Badger L, Bernstein D, Bohn R, De Vaulx F, Hogan M, Iorga M, et al. US government cloud computing technology roadmap, vol. I. National Institute of Standards and Technology; 2014. https://doi.org/10.6028/NIST.SP.500-293.
[22] KPMG Team. Cloud strategies for public sector in central and eastern Europe. KPMG Central and Eastern Europe Ltd; 2013.
[23] Velte AT, Velte TJ, Elsenpeter R. Cloud computing: a practical approach. 2010. ISBN: 978-0-07-162694-1, MHID: 0-07-162694-8.
[24] Pudjianto B, Hangjung Z. Factors affecting e-government assimilation in developing countries. In: 4th communication policy research, south conference. Sri Lanka: Negombo; 2009.
[25] Khan F, Zhang B, Khan S, Chen S. Technological leap frogging e-government through cloud computing," Broadband Network and Multimedia Technology, 4th IEEE International Conference. IEEE; 2011. p. 201–6.
[26] Alshomrani S, Qamar S. Cloud based e-government: benefits and challenges. Int J Multidiscip Sci Eng 2013;4(6):1–7.
[27] Kundra V. Federal cloud computing strategy. 2011.
[28] Varma V. Cloud computing for E-governance. A White Paper IIIT Hyderabad; 2010. http://www.iiit.ac.in/~vasu.
[29] Hashemi S, Monfaredi K, Masdari M. Using cloud computing for e-government: challenges and benefits, "World Academy of Science, Engineering and Technology, international science index 81. Int J Inf Sci Eng 2013;7(9):987–95.
[30] Almarabeh T, Majdalawi YK, Mohammad H. Cloud computing of e-government. Commun Netw 2016;8(1):1.
[31] Craig R, Frazier J, Jacknis N, Murphy S, Purcell C, Spencer P, et al. Cloud computing in the public sector," Public manager's guide to evaluating and adopting cloud computing. White Paper. Cisco Internet Business Solutions Group; 2009.
[32] The Open Cloud Manifesto Consortium. Draft 1.0.9. "The Open Cloud Manifesto". 2016. Retrieved February 1, 2016, from: http://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf.
[33] Macias F, Thomas G. Cloud computing concerns in the public sector: how government, education, and healthcare organizations are assessing and overcoming barriers to cloud deployments. 2011 [White paper]. [Retrieved from Cisco website: http://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf.
[34] Hashemi S. Cloud computing technology for e-government architecture. Int J Found Comput Sci Technol 2013;3(6).
[35] Tripathi A, Parihar B. E-governance challenges and cloud benefit. VSRD Int J CS IT 2011;1(1):29–35.
[36] Esteves J, Rhoda CJ. A comprehensive framework for the assessment of e-government projects. Gov Inf Q 2008;25:118–32.
[37] Armbrust B, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, et al. A view of cloud computing. Commun ACM 2010;53(4):50–8. ACM.
[38] Hana MA. E-government cloud computing proposed model: Egyptian e_government cloud computing. In: Advances in computing, communications and informatics, international conference. IEEE; 2013. p. 847–52.
[39] Karokola GR. A framework for securing e-government services: the case of Tanzania [Doctoral dissertation]. Department of Computer and Systems Sciences, Stockholm University; 2012.
[40] Kumar P, Kumar D, Kumar N. Improved service delivery and cost effective framework for e-governance in India. 2013.
[41] Almunawar MN. Benefits and issues of cloud computing for e-government. Rev Pub Adm Manag 2017;3:e105. https://doi.org/10.4172/2315-7844.1000e105.