Government Information Quarterly 28 (2011) 239–251

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Securing e-Government and e-Voting with an open cloud computing architecture

Dimitrios Zissis *, Dimitrios Lekkas

Department of Product and Systems Design Engineering, University of the Aegean, Ermoupolis, Syros, GR-84100, Greece

ARTICLE INFO

Available online 12 March 2011

Keywords:
Cloud computing
Electronic voting
Electronic government
Information and communication security

ABSTRACT

The idea, the concept, and the term, that is cloud computing, has recently passed into common currency and the academic lexicon in an ambiguous manner, as cloud dust is being sprinkled on an excess of emerging products. Exorcising complexity and protecting against the caprice of the moment, this paper explores the notion behind the hype of cloud computing and evaluates its relevance to electronic government and electronic voting information systems. This paper explores increasing participation and sophistication of electronic government services, through implementing a cloud computing architecture. From an Information and Communication Security perspective, a structured analysis is adopted to identify vulnerabilities, involved in the digitalization of government transactions and the electoral process, exploring the notion of trust and transparency within this context. In turn, adopting a cloud computing approach for electronic government and electronic voting solutions is investigated, reviewing the architecture within the previously described context. Taking a step further, this paper proposes a high level electronic governance and electronic voting solution, supported by cloud computing architecture and cryptographic technologies, additionally identifying issues that require further research.

1. Introduction

In the 1960s, few could have predicted the impact that an undersized academic network of four mainframe computers, residing at different universities and research centers, would have on the future of communications. This was the predecessor to today's internet, which currently has approximately 1.4 billion users worldwide (Wolfram Alpha, 2009). High speed internet connections (i.e. broadband connections) are now being perceived as a basic commodity in the global village's market, and are treated as key economic indicators. Information Systems (IS) and technological innovations have emerged as central actors responsible for storing, processing and providing accurate information on request. The global economy is being shaped through the demand on technological innovations and information systems, which in turn pressurizes the knowledge curve to constantly meet with the continuous shift in requirements.

At the dawn of the third millennium, countries and states around the world are exploring new frontiers by attempting to connect with their citizens through novel technologies. In relation to technological progress, exploring methods of increasing involvement in democracy and sovereign institutions has taken center stage, as electronic participation channels present a bi-directional communication gateway between the "people" and their elected representation. In these years, numerous information policies and instruments have made electronic governments a global reality. Since their initial introduction, electronic government services have been continuously maturing, evolving in both availability and sophistication. e-Governments have been progressing from an "initial online presence, through a limited number of individual governmental pages," towards a "totally integrated presence, which has the ability to cross departments and layers of government" (Capgemini, 2009). The EU Ministerial Declaration of 2009 (EU Ministerial Declaration on e-Government, 2009), in accordance with relevant initiatives globally (e.g. U.S. Federal Cloud Computing Initiative, 2009; e-Government Act of 2002, December 17, 2002; and Memorandum for chief information officers, 2007), determines the next generation of e-Government goals and objectives. This strategic plan is a multistep process aimed at overcoming economic, social, and environmental challenges, which, in turn, will lead to a more open, flexible, and collaborative electronic government. Improving collaboration between citizens and government agencies is critical to the success of these initiatives, as it will lead to increasing the efficiency and effectiveness of its services. Fulfilling these goals will provide economies of scale and knowledge for governments and society. Developing more inclusive services that will help bring down barriers experienced by digitally or socially excluded groups is identified as a necessity. These initiatives, which aim to provide better public services, are delivered with fewer resources by optimizing the use of available resources and instruments, while improving organizational processes and promoting a sustainable low-carbon economy.

The goals and objectives identified by EU'09 (EU Ministerial Declaration on e-Government, 2009) serve as a framework for

* Corresponding author.
E-mail addresses: D.Zissis@aegean.gr (D. Zissis), Dlek@aegean.gr (D. Lekkas).

0740-624X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.giq.2010.05.010

achieving successful progression to the next generation of electronic governments. Fig. 1 represents the goals and objectives (soft goals) identified in the EU'09 initiative.

Following a goal-driven methodology, this paper is structured around accomplishing the main goals identified in the EU'09 initiative and relevant regulations, including the improvement of collaboration in e-Government through increasing business interoperability and citizen participation, while achieving the objectives of openness, flexibility, and sustainability. The first section of this paper introduces a new technology and operational model for Information Systems (IS), cloud computing, and systemically explores the benefits gained from its application to e-Government. In the following section, electronic voting is introduced as a critical element for improving citizen collaboration through increasing citizen participation in the decision making process. As security is identified as the main barrier to the wide deployment of electronic voting IS, the notion of security is investigated within this context. Following a deductive analysis and extensive literature review, a number of information security threats and vulnerabilities are documented, leading to specific design principles essentially incorporated in a proposed solution. The research methodology that is adopted towards achieving this goal is based on software engineering and information systems design approaches. The basic steps for designing the system architecture include the collection of requirements and the analysis of abstract functional specifications. The collection of requirements and related functions is based on reviewing existing regulatory frameworks, such as those published by the National Institute of Standards and Technology (NIST) and other organizations. A systematic analysis of cloud computing, once it is weighed against identified requirements, leads to the proposal of a high level electronic governance and electronic voting solution, supported by cryptographic technologies. Additionally this paper identifies issues related to cloud computing which require further research.

2. Literature review

Several concepts that are used throughout the manuscript are discussed in this section, including electronic democracy, electronic voting and electronic participation. The first section of this paper then goes on to introduce a new technology and operational model for Information Systems (IS), cloud computing, and systemically explore the benefits gained from its application to e-Government.

2.1. Introduction of terms electronic democracy and e-Voting

Since the publication of "the nerves of government" (Deutsch, 1963), information and communication technologies (ICT) have been considered vital for political systems. Information and communication technologies were recognized to have tremendous administrative "potential" (Yildiz, 2007), and ICTs could help create a networked structure for interconnectivity (McClure & Bertot, 2000), service delivery (Bekkers & Zouridis, 1999), efficiency and effectiveness (Heeks, 2001a,b), interactivity (DiCaterino & Pardo, 1996), decentralization, transparency (La Porte, De Jong, & Demchak, 1999), and accountability (Ghere & Young, 1998; Heeks, 1998, 1999; McGregor, 2001).

e-Government is defined as "utilizing the internet and the world-wide-web for delivering government information and services to citizens" (UN&ASPA—United Nations/American Society for Public Administration, 2002). In addition to the internet and the web, e-Government may also include using other ICTs such as "database, networking, discussion support, multimedia, automation, tracking and tracing, and personal identification technologies." (Jaeger, 2003,

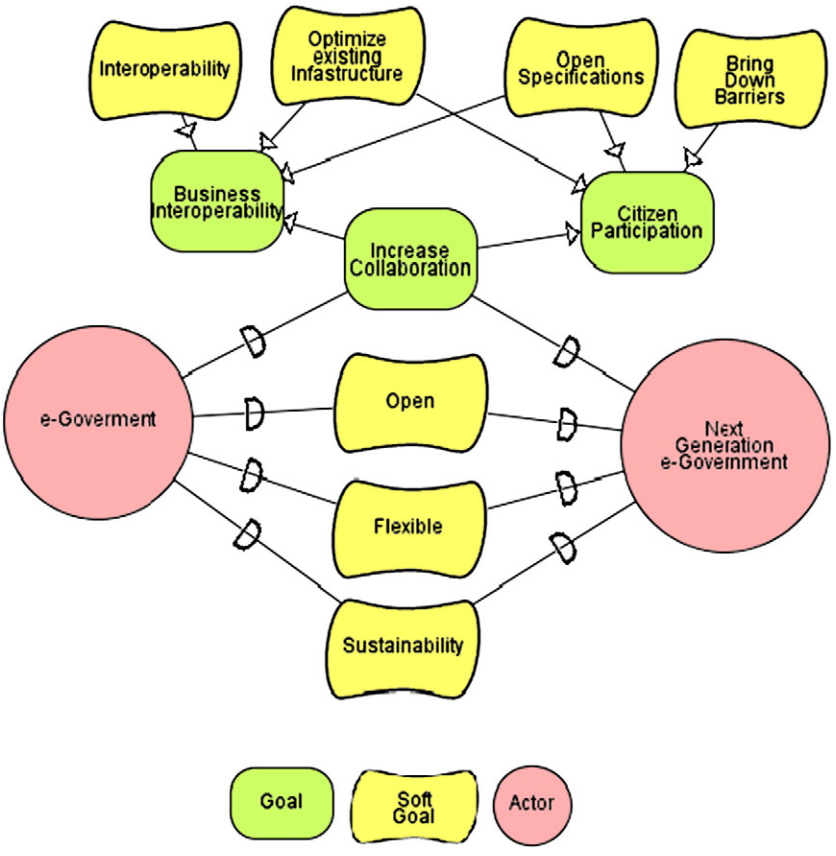

Fig. 1. Goals and objectives (soft goals) identified in the EU'09 initiative.

p. 323). Electronic democracy is identified as the *electronic* representation of democratic processes (Von Lucke & Reinermann, 2004), which in turn are divided into three sub-processes (Parycek, 2003):

- Acquisition of information,
- Formation of an opinion, and
- The decision itself.

Empowered by timely information and by deliberations of the discursive community, citizens may effectively participate in decision making processes, for example e-Referenda. The internet can be perceived as an evolution of current communication linkages between political representatives and citizens. The process of using ICT to engage the public in democratic processes is named electronic participation. e-Participation can be understood as technology-mediated interaction, between the civil society sphere and the formal politics sphere and between the civil society sphere and the administration sphere (Clive Sanford, 2007). The task of e-Participation is to empower people with ICT so as to be able to act in bottom-up decision making processes, to make informed decisions, and to develop social and political responsibility. Therefore, e-Participation is a means of empowering the political, socio-technological, and cultural capabilities of individuals and affording people the opportunity to involve and organize themselves in the information society (Fuchs, Bernhaupt, Hartwig, Kramer, & Maier, 2006).

It is apparent that the terms electronic democracy and electronic voting are interoperably linked. Electronic voting is a vital and indispensable aspect of electronic democracy. Electronic voting has the capacity to engage citizens in a wider spectrum than what is currently available in a conventional electoral process. Electronic voting (e-Voting) provides citizens with a means to express their timely opinion on civil affairs involving, for example, legislation, election of representatives, etc. Currently, a universally acceptable definition for e-Voting is lacking. The term is being ambiguously used for a variety of IS with a wide spectrum of tasks, ranging from vote casting over electronic networks to electronic voter registration.

In general, two main types of e-Voting can be identified (Buchsbaum, 2004):

- *e-Voting*: Voting is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines at polling stations or municipal offices, or at diplomatic or consular missions abroad); and
- *Remote e-Voting*: Voting is within the voter's sole influence, and is not physically supervised by representatives of governmental authorities (e.g. voting from one's own or another person's computer via the internet (i-voting), by touch-tone telephones, by mobile phones (including SMS), or via Digital TV, or at public open-air kiosks — which themselves are venues and frames for different machines, such as PCs or push-button voting machines, with or without smart card readers).

In this paper, the term e-Voting is used to represent remote electronic voting performed within the voter's sole influence (remote internet voting).

Despite controversies surrounding e-Voting, electronic voting systems are gradually replacing traditional paper-based ones, in many countries. Numerous governments are currently in the process of evaluating electronic voting solutions. They are holding a succession of trials and pilots to determine the benefits and drawbacks offered by their deployment. Electronic voting enables citizen deliberation, by providing a method for efficiently expressing timely opinion on matters of state, thus improving citizen's participation in the democratic processes. e-Voting provides a macroeconomic, cost-efficient method for increasing election accuracy and efficiency. Additionally, by escalating usability and accessibility, these Information Systems aim at increasing transparency and openness in democracy.

As an increasing number of countries and states consider implementing e-Voting systems, electronic voting security has become an all important issue, as concerns over privacy and confidentiality issues are often raised. It is a common fact that back-end computers are already an integral part of almost all elections held internationally. Even in countries not officially exploring electronic voting, back end computer systems are most possibly introduced at some stage of the electoral process, either for ballot counting or for voter list generation. These back-end "uncertified" computers hold more dangers than an efficiently designed and protected electronic voting system. e-Government and e-Voting IS's handle an immense amount of critically sensitive information, which requires the preservation of data confidentiality, integrity, and availability, at all costs. Additionally, system security should guard the principles of authenticity and uniqueness of data, and implement non-repudiation of communications. Novel solutions are constantly explored to counteract these imminent threats.

2.2. Cloud computing

Throughout computer science history, numerous attempts have been made to shift users from computer hardware needs and from time-sharing utilities envisioned in the 1960s and the network computers of the 1990s to the commercial grid systems of more recent years. This abstraction is steadily becoming a reality as a number of academic and business leaders in this field of science are spiraling towards cloud computing. Cloud computing is an innovative IS architecture, visualized as what may be the future of computing, a driving force demanding from its audience to rethink their understanding of operating systems, client server architectures, and browsers.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (National Institute of Standards and Technology (NIST), 2009). The name cloud computing was inspired by the cloud symbol that is often used to represent the internet in flow charts and diagrams. A distinct migration to the clouds has been taking place over recent years with end users maintaining a growing number of personal data, including bookmarks, photographs, music files, etc. on remote servers accessible via a network.

Cloud computing is empowered by virtualization technology, a technology that actually dates back to 1967, but that for decades was available only on mainframe systems. In its quintessence, a host computer runs an application known as a hypervisor; this application creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications (Naone, 2009). The software "supposes" it has physical access to a processor, network, and disk drive. Virtualization is a critical element of cloud implementations and is used to provide the essential cloud characteristics of location independence, resource pooling, and rapid elasticity (explained in detail in the following section). Differing from traditional network topologies (e.g. a client server), cloud computing is able to offer flexibility and alleviate traffic congestion issues.

At a low level, a hardware layer, a number of physical devices, including processors, hard drives and network devices, are located in data centers, independent from geographical location, which are responsible for storage and processing needs. The combination of software layers, the virtualization layer, and the management layer allows for the effective management of servers. The virtualization layer allows a single server to host many virtual servers, each of which can operate independently of the others. The management layer monitors traffic and responds to peaks or drops with the creation of new servers or the destruction of non-necessary ones.

Beyond the software layers are the available service models, which are:

1) *Infrastructure as a Service (IaaS).* IaaS provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications.
2) *Platform as a Service (PaaS).* PaaS provides the consumer with the capability to deploy consumer-created or acquired applications, which are produced using programming languages and tools supported by the provider, onto the cloud infrastructure.
3) *Software as a Service (SaaS).* SaaS provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g., web-based email).

Four deployment models have been identified for cloud architecture solutions and are described below.

1) *Private cloud.* The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.
2) *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.
3) *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4) *Hybrid cloud.* The cloud infrastructure 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 (e.g., cloud bursting for load-balancing between clouds) (NISp & Peter Mell, 2009).

Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues. A number of key characteristics of cloud computing have been identified (Sun Microsystems, 2009; Reese, 2009; NISp and Peter Mell, 2009; Buyya, Yeo, & Venugopal, 2008; Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009; Peter Mell, 2009):

1) *Flexibility/elasticity.* Users can rapidly provision computing resources, as needed, without human interaction. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out or up.
2) *Scalability of infrastructure.* New nodes can be added or dropped from the network as can physical servers, with limited modifications to infrastructure set up and software.
3) *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms (e.g., mobile phones, laptops, and PDAs).
4) *Location independence.* 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.
5) *Reliability.* Reliability improves through the use of multiple redundant sites, which makes cloud computing suitable for business continuity and disaster recovery.
6) *Economies of scale and cost effectiveness.* Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located close to cheap power stations and in low-priced real estate in order to lower costs.
7) *Sustainability.* Sustainability comes about through improved resource utilization, more efficient systems, and carbon neutrality.
8) *Open free software.* The need for openness and interoperability is a driving force for designing and implementing cloud infrastructures, and for moving towards open source software solutions. The massive scale of many clouds, combined with the need for many software licenses, encourages the use of free software in the development of cloud architectures. To prevent vendor lock-in, open APIs, open data formats, and standards implemented through open-source reference models are vital requirements.
9) *Advanced security technologies.* Cloud implementations often contain advanced security technologies, which are mostly available due to the centralization of data and universal architecture. The homogenous, resource-pooled nature of the cloud enables cloud providers to focus all of their security resources on securing the cloud architecture. At the same time, the automation capabilities within a cloud, combined with the large focused security resources, usually result in advanced security capabilities.

Maintaining a perspicacious vision is essential in a field that is evolving exponentially. Cloud computing is not a panacea and many believe it to be little more than market-driven hype. Cautiousness is necessary, so as not to be carried away by the caprice of the moment. In its quintessence, cloud computing has the capability to address a number of identified deficiencies of traditional architectures. Progress requires its audience to rethink their understanding of solid notions such as, the network and personal computers.

3. Meeting the first goal-increasing collaboration between agencies and federal institutions

Public sector processes are often regarded as problematic, as concerns are expressed of delay, mismanagement, and dysfunctionality, all of which contribute to the inefficiency of public services. The explosion of the internet and the rapid e-Government push brought many of these problems online. Diversity of tools and data formats between agencies and business partners led to the degeneration of data quality and accuracy used in transactions with e-Governments. In addition, the variety of tools employed deteriorated cooperation and generated cross-agency collaboration barriers. Research has shown that these selections also took their toll on end users, as usability of public services declined through their diversity and complexity (Wimmer, 2002; Verdegem & Verleye, 2009). There is a growing expectation from citizens and businesses for their governments to be more open, flexible, and collaborative. ICT has reached a level of impact that goes well beyond technological boundaries; it is identified as an important enabler capable of delivering policy goals across different sectors, widening collaboration, increasing administrative efficiency and effectiveness, and bridging social diversities. Electronic government policies need to contribute to making the benefits of ICT reach the people, by providing more feasible and efficient solutions that improve citizen, intergovernmental and business access to information, and services by supporting interoperability and collaboration. A systemic approach is required, which will ensure interoperability by implementing standards which enable cooperation, while supporting these attempts by incorporating into the country's legal system suitable measures relating to ICT.

Recently, the U.S. federal cloud computing initiative was published, which is a service oriented approach, whereby common infrastructure information and solutions can be shared across the U.S. government (National Institute of Standards and Technology (NIST), 2009). The overall objective is to create a more agile federal enterprise using cloud computing architecture by which services can be reused and provisioned on demand to meet business needs. This endeavor can be viewed as an opening step into computing clouds, which is primarily focused on applications dealing with less sensitive data.

These initiatives hold the capacity to expand into the building blocks of a universal e-Government solution supported by cloud infrastructure, whereby computing resources and tools can be uniformly shared between agencies and citizens while increasing participation.

The U.S. federal cloud computing initiative provides a high-level overview of the key functional components for cloud computing services for the government.

- Citizen adoption (Wikis, blogs, social networking, collaboration and participatory tools)
- Government productivity (email/IM services, office automation etc.)
- Government enterprise applications (business applications, core mission applications, and legacy applications)

As initiatives across the globe are attempting to improve organizational processes and cooperation between federal institutions and businesses, it is crucial to unify tools and infrastructure into a common platform. Cloud computing offers an operational model that can digitally amalgamate geographically remote data centers into a common infrastructure, providing a principal gateway to government related services and data. Cloud computing leverages existing infrastructure and provides public services while using fewer resources, reducing carbon emissions, and contributing to wider carbon-reduction targets.

Federal institutions adopting a cloud computing operating model benefit from the concentration of data; centralization leads to greater consistency and accuracy. Unifying remote data centers into a universal solution overcomes problematic issues of data consistency, (federal agencies maintaining out-dated archives, several data formats in use etc.). The risks that are involved with the adoption of proprietary software and data formats for the long term survival of data are enormous. The adoption of proprietary standards and software models, which lock data into a specific model, can jeopardize system security, privacy, and interoperability. The creation of a truly competitive computing marketplace that allows for portability and easy switching between providers requires a triumph of open APIs, open data formats, and standards that are implemented through open-source reference models (Wardley, Goyer, & Barcet, 2009).

The centralization of data and application solutions holds the capacity to provide additional tools, thereby enhancing timely communications and control. Reducing the time required to access both data and applications, not only across the federal structure but also between business partners, generates stronger collaboration. Leveraging existing remote infrastructures into a common IS reduces installation and monitoring time and expenses, and focuses on improving quality. By centrally managing, developing, implementing, and assessing IS's costs can be amortized across the federal structure.

It is imperative to follow a methodological framework for the assessment and analysis of electronic government proposals, as there are many technical, organizational, and institutional elements to be considered. This paper adopts a framework proposed by Montagna (2005), which enhances previous works done by several scholars, that allows determining whether proposed initiatives are suitable for governmental action and determines the benefits provided in a multidimensional approach. This framework also evaluates initiatives regarding the dimensions characterizing e-Government actions, products (Table 1), time (Table 2), distance (Table 3), interactions (Table 4), and procedures.

Adopting a cloud infrastructure for electronic government presents a number of business drivers.

1) *Performance.* The cloud computing model increases cross-agency collaboration, as tools and data can be deployed upon demand, reducing any additional overhead. Business and citizen related tasks can benefit from increased computational resources, available due to the elasticity of cloud computing services. The architectural characteristics can support the deployment of additional "citizen to citizen" and "business to business" tools, which can increase participation and electronic governance performance. The centralization of data, improves data quality and availability, increasing the efficiency of related business processes.
2) *Cost efficiency.* Cloud computing proposes many cost effective gains and business drivers. Cloud computing deployments benefit from economies of scale, as purchasing hardware is performed in a large scale and data centers can be deployed at geographical locations, with lower overheads, (such as real estate, electricity, etc.). Due to the elasticity of services provided, energy efficiency and power savings reduce overall expenditure. The cost of human resources may additioally be reduced, as it will not be required for all agencies to staff technical teams and powerful management automation characteristics can alleviate the load put on administrative teams. Furthermore, the use of open source software solutions can minimize costs, which, in turn, can reduce the need for multiple licenses in the cloud.
3) *Scalability.* In addition to cloud infrastructure's ability to scale to demand, either horizontally or vertically though virtualization, hardware servers can be added to the infrastructure in a complex free manner.
4) *Resiliency and business continuity.* Deploying data centers at multiple geographical locations – often referred to as availability zones – guarantees availability of services, if a specific data center fails. In the instance of a disaster, sophisticated network rerouting ensures business continuity.
5) *Maintainability.* Centralization of IT infrastructure simplifies monitoring and maintenance tasks.
6) *Security.* The cloud computing model provides a plethora of information and communication security benefits, including centralization and unification of the security infrastructure.

Table 1
An evaluation of cloud computing in relation to electronic government.

Performance criteria	Product
Efficiency	–Provides uniform access to data and applications
Effectiveness	–Improves data quality –Improves quality of services
Strategic benefits	–Provides uniformity of solution –Introduces new services –Integrates existing infrastructure deployments
Transparency	–Constant evaluation and control of services and application usage, reduction of expenses

4. Achieving the second goal: Increasing citizen participation by enabling secure electronic voting

This section explores increasing citizen participation in governance by enabling electronic voting. As electronic voting security is essentially identified as the main barrier to the wide deployment of electronic

Table 2
An evaluation of cloud computing in relation to electronic government from the perspective of "time".

Performance criteria	Time
Efficiency	–Reduces time required to access applications and data –Reduces time required for installations and modifications –Reduces monitoring time
Effectiveness	–Applications and resources available on demand
Strategic benefits	–Timely opinion and expression –Possibility of real time cooperation across agencies
Transparency	–Timely control

Table 3
An evaluation of cloud computing in relation to electronic government from the perspective of "distance".

Performance Criteria	Distance
Efficiency	–Overcomes geographical difficulties –Crosses agency and boundaries cooperation –Reduces distribution and delivery cost –Improves data quality due to centralization and uniformity –Improves data accuracy due to centralization and uniformity
Effectiveness	–Improves communication and interaction
Strategic benefits	–Introduces new services independent of geographical location –Hybrid centralization
Transparency	–Access services and data independently from geographical location

voting IS, the notion of security is investigated within this context. Following a deductive analysis and extensive literature review, a number of information security threats and vulnerabilities are documented, leading to specific design principles essentially incorporated in a proposed solution, along with recommendations of considerations that can assist in reducing these threats and vulnerabilities

4.1. Increasing citizen participation with cloud computing

Cloud computing has the capability to evolve beyond meeting the business needs of e-Government agencies and towards providing to numerous identified e-Citizens related shortages. In the 1960s John McCarthy, speaking at the MIT Centennial, stated that computation may someday be organized as a public utility "Cloud computing is a reincarnation of the computing utility of the 1960s but is substantially more flexible and larger scale than systems of the past", says Google executive and internet pioneer Vint Cerf. The vision of computing, offered to all, when paired with initiatives such as e-Inclusion and One Laptop Per Child, presents an opportunity to overcome economic disparities and geographical differences in society, steering towards an all-inclusive digital e-Citizen platform.

The appearance of cloud computing demands that we rethink our current understanding of personal computers, operating systems, and network architectures. Clusters of web servers assembling, conjuring clouds of massive computational resources, could inevitably one day meet all individuals' needs. The opportunities for e-Government are enormous, and providing a personalized online desktop system, which would be accessible via a "web browser" or a custom-made operating system, is just around the corner. Barriers to the wide adoption of e-Government solutions may be abolished all together, as purchasing hardware to upgrade a personal computer to meet with growing requirements may one day be a remnant of the past, as all computational needs could be met through a "dumb" terminal over a network. Clouds can enhance electronic participation by providing the means for wider citizen involvement, bringing down barriers experienced by digitally or socially excluded groups.

Cloud computing provides a single access point towards a gateway of interaction with government information, personal information and government representatives, presented through an online desktop application for all citizens. Through SaS, a surplus of applications can be provided, including social networking and collaboration tools, cryptographic functions, electronic voting functions, information services, email, etc., thereby linking supportive infrastructure with services supplied.

Table 4
An evaluation of cloud computing in relation to electronic government from the perspective of "interactions".

Performance criteria	Interaction
Efficiency	–Reduces deployment cost –Reduces interaction costs –Increases cooperation –Increases participation
Effectiveness	–Generates relationships –Enhances accessibility
Strategic benefits	–Builds new communication and operation channels –Offers more information and increases the accuracy of information available
Transparency	–Promotes active participation –Breaks down barriers

4.2. The importance of enabling secure e-Voting

An abundance of global initiatives are focusing on increasing citizen–government collaboration. Collaboration in this context is defined as a recursive process where citizens and federal institutions cooperate in an intersection of common goals. To achieve this goal, mechanisms for effective citizen participation are constantly being explored "in order to complement the know-how of government employees with the expertise and intelligence of the people" (Open Government Iniative, 2009).

As e-Government solutions meet the initial needs of information acquisition and formation of an opinion, a shift of focus is occurring towards the next aim of e-Democracy: expression of opinion. What is currently lacking from most electronic government information systems is the capacity to support effective citizen participation in the decision making process, beyond the electronic implementation of traditional bureaucratic services. Voting represents the most vital citizen participation process in democracy; it can inherently facilitate the expression of general will. Enabling secure electronic voting strengthens electronic democracy, as it targets increasing deliberation in a bottom up method. The ultimate goal for all e-Government attempts is the digitization of this process, so as to offer citizens a timely, location-independent, and transparent means of participation in governance.

Electronic voting is envisioned as having the capacity to introduce many advantages to the electoral process, which include widening access to the voting process for people with disabilities, increasing turnout, reducing time and cost of elections, and providing a more reliable service (Council of Europe, Committee of Ministers, 2004). Remote electronic voting offers the same advantages as (poll-site) electronic voting while adding (Riera & Brown, 2003) cost reductions due to economies of scale and increased participation due to voter geographic independence.

The security aspect in the context of the electoral process is referred to as one of the most important constraints in the adoption of electronic voting systems. The Caltech-MIT Voting Technology Project states: "Security is as important as reliability in guaranteeing the integrity of the voting process and public confidence in the system. Losing confidence in elections means losing confidence in our system of government." (MIT, 2001). The e-Government Act of 2002 recognized the importance of information security to the economic and national security interests of the United States. Fuelling concerns, a report published by a panel of IT security experts, which reviewed the SERVE Interent Voting System, concluded that given the state of the internet and PC hardware, vulnerabilities existed that could not be overcome, so the deployment of e-Voting should be aborted (Jefferson, Rubin, Simons, & Wagner, 2004).

A *vulnerability* is a weakness in an IS system that can be exploited by an attacker interested in penetrating a system. IS security blocks threats on a system by *controlling* a vulnerability; this is a defensive measure that reduces or eliminates a given vulnerability. Although a single security mechanism is generally insufficient as no control must be considered a gold standard, a layered solution is able to control a plethora of vulnerabilities. Security mechanisms (defenses) need to be layered so that compromise of a single security mechanism is insufficient to compromise an entire host or network; this is referred

to as Defense in Depth. A number of controls and countermeasures have been regulated by NIST, specifically for the protection of federal information systems. The e-Government Act 2002 (the full title for which is the Federal Information Security Management Act of 2002 (FISMA)), tasked NIST with responsibilities for standards and guidelines, including the development of guidelines, the recommendation of types of information and information systems to be included in each category, and the recommendation of minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each category (NIST SP 800-53, 2008; NIST SP 800-53A, 2008; NIST SP 800-59, 2003).

Electronic voting security includes a wide spectrum of fields, procedures, issues, and actors which are relative to the technological approach taken. It effectively relates to the procedures and standards that are put into place to overcome technological security shortcomings (Mohen & Glidden, 2001; Williams, 2004; Xenakis, 2004). Decisions made regarding system characteristics and elements are crucial to the success of such systems and guide design through the implementation of the identified technologies. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems' engineering process to effectively integrate the security controls with the information systems' functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability) (NIST Special Publication 800-60, 2008).

Currently, a number of cryptographic schemes attempt to provide a sense of security in e-Voting. Cryptographic protocols provide an opportunity to generate trust between involved parties of an election. Because it deals with the integrity, confidentiality, and authenticity of communications and data, cryptography is a crucial element in the overall system security. Unfortunately, a wide number of threats to e-Voting security can circumvent cryptographic solutions before they have been applied. With traditional hardware and software architectures, a malicious payload on a voting client can modify the voter's vote, without the voter or anyone else noticing and regardless of the kind of encryption or voter authentication in place. Essentially, because the malicious code can do its damage before the encryption and authentication is applied to the data, the malicious module can then erase itself after doing its damage so that there is no evidence and no way to detect the fraud. Although strong encryption is a very powerful tool for addressing issues of integrity, confidentiality and authenticity, additional technological implementations are required to address availability issues and enhance overall computer security.

4.3. Identification of security requirements for electronic voting

e-Voting security is in effect a matter of trust. Deconstructing the perception of trust within the context of e-Voting IS leads to the formation of a framework for generating and maintaining the necessary security properties. Essentially, software is believed to be "trusted" if the source code has been rigorously developed and analyzed, both of which give us reason to believe that the code does what it is expected to do and nothing more. Within the boundaries of e-Voting, a trusted IS needs to address the issues of:

- Ensuring that the voter is provided with the means to cast his or her vote.
- Ensuring that the voter is prevented from casting more than one valid vote.
- Ensuring that the cast ballot is confidential in the sense of not being linked to the voter who cast it.
- Ensuring that the vote may not be changed or faked.
- Ensuring that votes are not lost.
- Ensuring that no votes are entered that have not been cast by authorized voters.

Breaking down the concept of security and sequentially mapping requirements to key trust characteristics, generates a list of requirements and vulnerabilities, which must be controlled by a proposed solution.

1) *Availability* refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a system's ability to carry on operations even when some authorities misbehave. The system must have the ability to continue operations, even during a security breach. In the context of e-Voting systems, this property refers to legitimate voters provided with the means to cast their vote. Safeguarding this security requirement denotes implementing the technological solutions to protect the system against network attacks, which would make the system unavailable to end users.
2) *Confidentiality* refers to only authorized parties or systems having the ability to access protected data. In the context of elections it refers to data and voter preferences remaining private. An election is private, if neither the election authorities nor anyone else can link any ballot to the voter who cast it, and no voter can prove that he or she voted in a particular way.[1]
3) *Integrity* refers to data and system precision, accuracy, and consistency. Votes must be recorded correctly and safeguards must ensure that votes cannot be modified, forged or deleted, without detection. In elections, all data involved in entering and tabulating votes must be tamperproof. Reliability is fundamental, as it means that an election system should work robustly, without the loss of any votes, as well as dependably and accurately. Integrity refers to the system, data, and to personnel. People involved in developing, operating, and administering electronic voting systems must be of unquestionable integrity.
4) *Authenticity* refers to the assurance that the involved data, transactions, communications, and/or documents (either electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. In elections it is vital that only registered voters are permitted to cast a vote. The voting must be protected from external reading during the voting process. Voter identity and preferences must be kept secret.
5) *Accountability* refers to information, selectively kept and protected, so that actions affecting security can be traced back to the responsible party (audit). Corrupt voters or personnel may attempt to modify votes, the voting count, or the system. Also related to accountability is system disclosure, which refers to system software, hardware, microcode, and any custom circuitry being open for random inspection and documentation at any time, despite cries for secrecy from the system vendors. The property of permitting an external auditing entity, but also a voter, to verify that votes have been counted correctly, is crucial. All internal operations must be monitored, without violating voter confidentiality, and all operator authentication operations must be logged.

Together, availability, confidentiality, integrity, authenticity, and accountability refer to safeguarding a system against the threats listed in Table 5.

4.4. Proposed solution

In the field of computer and network security the principle of the weakest link is often quoted. This principle states that overall system security cannot be stronger than its weakest link. As security is often viewed as a chain, a single breaking point will crumple its efficiency. An intruder must be expected to use any available means of

[1] An important confidentiality issue is the concern of coercion and prevention of vote buying ensured by an e-voting system. Although solutions seem to have the ability to address this issue, it is out of the scope of this paper and is not addressed. Coercion must be addressed at an application and procedure level.

Table 5
Protecting availability, confidentiality, integrity, authenticity, and accountability of a system refer to safeguarding against the threats listed in this table.

	Availability	Confidentiality	Integrity	Authenticity	Accountability
Connection flooding	x				
DDOS	x				
DNS attack	x		x		
Eavesdropping		x		x	
Exposure within network		x			
Falsification of messages			x		
Hardware interception	x	x	x		x
Hardware modification	x	x	x		x
Hardware substitution	x	x	x		x
Impersonation/spoofing			x	x	
Malicious code on client	x	x	x		
Man in the middle—*Replay*		x	x	x	
Misdelivery		x			
Software modification					
EasterEggs		x	x		x
Information leaks		x	x		x
Logic bombs		x	x		x
Trojan horse		x	x		x
Virus		x	x		x
Trapdoors		x	x		x
Session hijacking		x		x	
Software deletion		x	x		
Software theft		x			x
Traffic flow analysis		x			
Traffic redirection	x			x	
Wiretapping		x	x		

penetration and shall attack a system at its most vulnerable point. The client's personal computer is identified as the weakest point in an e-Voting environment (Jefferson et al., 2004; Gritzalis, 2002; Cranor, 2003). Voters' home computers are most likely to be less defended than corporate ones, as they often run outdated virus protection systems, misconfigured firewalls, unpatched operating systems, and contain numerous applications from various vendors, making these machines especially susceptible to malicious attacks. The NIST guide to "Enterprise Telework and Remote Access Security guide for Federal IS" NIST SP 800-46 (2009) states that the primary threat against most telework client devices is malware, including viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. Election integrity is closely related to the integrity of the terminal over which the voters vote is cast (Gritzalis, 2002).

A number of requirements have previously been proposed to guard the integrity of the client's terminal (Gritzalis, 2002):

- Users should administer the system only from specific terminals, within a predefined time window, using a combination of strong authentication means, such as biometrics or smart cards.
- The minimum necessary software and hardware components should be installed on the host of the voting system.
- The maximum possible level of operating system security enhancement should be applied to all machines of the voting system.

Additionally, the NIST guide to enterprise telework and remote access for Federal Information Systems states that, "telework client devices should have the same local security controls as other client devices in the enterprise — OS and application security updates applied promptly, unneeded services disabled, antimalware software and a personal firewall enabled and kept up-to-date, etc" (NIST 800-46, p. 4-2).

This paper proposes enabling electronic vote casting by minimizing threats through offering "desktop as a service" (a container of a collection of virtual objects, software, hardware, configurations etc., residing on the cloud, used by a client to interact with remote services). Leveraging existing infrastructure into a dynamically responsive cloud overcomes several deficiencies of traditional implementations. Providing citizens with "hardened" operating systems (OS), on a bootable read-only removable media, with preconfigured cloud access client software, eliminates a plethora of threats. A user can bypass loading a PCs vulnerable OS by inserting a preconfigured OS on removable media, thereby overstepping both compromise and threat. Authenticating a client over a secure channel, for a time-limited session required to perform vote casting, provides a control to a severe vulnerability.

Cloud computing places the user's terminal within the systems' "security perimeter", which is maintained, updated, and monitored by security experts. Due to its identified characteristics, cloud computing architecture attempts to propose an effective and efficient way of countering a plethora of threats, identified as barriers to electronic voting. In collaboration with a deployed Public Key Infrastructure (PKI), which serves as an authentication and cryptographic layer, cloud computing offers the benefits of placing the voter inside the "security perimeter". Enabling e-Voting through "desktop as a service" makes developing and maintaining common information security foundations an achievable goal. Centralization of security is crucial, as it provides a uniform and consistent way to manage the risk to individuals, organizational operations, organizational assets, whole organizations, and entire nations, from the operation and use of information systems (NIST SP 800-53; NIST Draft SP 800-39, 2008). Additionally, by centrally managing the development, implementation, and assessment of the common security controls, designated by the organization, security costs can be amortized across multiple information systems.

A cloud unique desktop as-a-service has the following characteristics:

- It is centrally maintained and monitored as part of a uniform protection scheme, which puts "client computers" behind professional security protection hardware, software, and personnel.
- Only authorized and authenticated software can be executed on the desktop instance due to management restrictions that can prevent many threats.
- Updates are rolled out centrally, increasing effectiveness and time of deployment.
- It is transparent and open to scrutiny.
- All source code used in the electoral process is contained for inspection.
- Policies and procedures are in place to protect from insider attacks, corruption, and hardware and software failures.

Documented below are recommendations of controls that can assist in reducing a number of previously identified threats and vulnerabilities (Table 6) (Pfleeger & Pfleeger, 2006; National Institute of Standards and Technology (NIST), 2009; Sun Microsystems, 2009; Reese, 2009; Peter Mell, 2009). These baseline security controls are, at most, in accordance with the tailoring guidance provided in NIST Special Publication 800-53 (2007), NIST Draft SP 800-39 (2008) and, generally speaking, they meet the OMB definition of adequate security for federal information systems, although a number of restrictions do not apply in a cloud environment. During their initial publication, cloud computing deployment models had not been considered; to amend this, NIST is planning a series of publications.

Controls and countermeasures deployed through the adoption of cloud computing architecture attempt to counter previously identified threats.

4.4.1. Controlling hardware-specific threats

On many occasions, attacks on sophisticated information systems have boiled down to deliberate assaults on hardware equipment. An attack against an electronic election could essentially be carried out by destroying the physical servers used in an election. A key characteristic of cloud architecture is geographical independence. The lack of knowledge of a server's location provides an interesting physical security benefit, as it becomes nearly impossible for a motivated attacker to use a physical vector to compromise the system. Additionally, data dispersal in the cloud "slices" information through sophisticated algorithms and stores data across different geographical locations. These technological characteristics contribute to high redundancy and availability achieved in the cloud (Reese, 2009).

High risk cloud infrastructures have the ability to realize distinct but overlapping availability zones. An availability zone can be conceptually mapped to a physical data center, with the security feature of having distinct physical infrastructures. Spanning virtual servers on multiple availability zones achieves geographical redundancy. Virtualization technology enables the inexpensive generation of redundancies, which span data centers and enable rapid recovery in the occurrence of disaster.

4.4.2. Controlling software-specific threats

Personal computers are often overloaded with software, developed by many different vendors. At any point an employee could consciously leave a backdoor, thereby creating opportunities for attacks against an electronic voting system. Backdoors, when placed in software, could be activated when a user tries to cast a vote (time-bombs), thereby invisibly monitoring or subverting the voting process. Providing a certified hardened OS on a bootable media, creates a secure thin client, open to extensive audits, generating unparalleled client side trust. This thin client would then be used to access the remote cloud desktop. In the cloud, it is possible to forbid uncertified software modifications, as updates and installations would be performed centrally to avoid threatening the systems integrity. Additionally, software installations can be restricted at a management level, eliminating the threat of installing malicious software on the system. In the event of a successfully deployed attack that modifies/deletes a voter's vote, all implicated software is contained and open to extensive audits. It is a fundamental requirement of an e-Voting system that all operations related to electronic voting, be logged and monitored (Gritzalis, 2002). A remote desktop on a cloud computing infrastructure (virtual instance), government owned and centrally monitored, would be open to extensive audits and to public scrutiny due to the adoption of open APIs, open data formats and open source models (Wardley at al., 2009).

In addition to the risk from pre-installed applications, there is a threat from remote attackers. Such an attacker might gain control of a computer without being detected. For example, an attacker could exploit security vulnerability in the software on a voter's computer. One of the identified benefits of cloud computing is the centralization of information and uniformity of security infrastructure, which can offer the ability to accurately address identified vulnerabilities across all clients. In addition, providing a "desktop within the clouds," makes it possible to overcome the exploitation of any vulnerability that could have been identified on a standard bootable OS or on the application contained within it. Updates can be rolled out effectively, as soon as the vulnerability has been identified, overcoming the drawback of "publishing day to update". The cloud provides a user interface that allows both the user and the IT administrators to easily manage the provisioned resources throughout the life cycle of the service request, effectively changing the installed software; removing servers; increasing or decreasing the allocated processing power, memory, or storage; and even starting, stopping, and restarting servers. These are self-service functions that can be performed 24 h a day and take only minutes to perform. By contrast, in a non-cloud environment, it could take hours or days for someone to have a server restarted or hardware or software configurations changed (IBM, 2009).

An attacker could attempt to exploit a vulnerability identified in a web server. In a traditional data center, rolling out security patches across an entire infrastructure is time consuming and risky. Due to the virtualization characteristics of cloud computing, increased efficiency is achieved. Virtual servers or instances are launched from a machine image. A machine image is a prototype which is copied onto a virtual server's hard drive every time an instance is launched. Updates and modifications are performed on a single image, which is successfully used to re-launch the virtual servers. In the cloud, rolling out a patch or update across the infrastructure takes three steps:

- Patching of machine images with new security updates,
- Testing the results, and
- Re-launching virtual serves.

Virus attacks impose an immense threat to such a system and traditional antivirus software would not be able to efficiently defend the system from such attacks. Specific antivirus tools can be provided as an additional cloud service to enhance end users' security coverage. A pure cloud antivirus solution relies on a detection set that resides on internet servers, or "in the cloud". A lightweight desktop agent is used to query this detection set. e-Voting systems are targets of system-specific viruses; it is imperative that effective solutions are created that can immediately deal with identified malicious code, preventing the propagation throughout the system. Cloud antivirus programs reduce the publishing delay to zero and allow for quicker innovation. They are more efficient and faster, providing security experts the ability to fine-tune their detection logic. After the identification of malicious code, server images can be hardened to protect against it and new server instances loaded. A proposed solution makes use of a Network Identification System and a centralized Host Intrusion Detection System which respectively monitors the system servers and network for anything unusual.

4.4.3. Controlling network specific threats

Attacks can be directed at a network's availability, or one of its services, but normally such attacks are focused on any IT services of which the network is an agent. Common attacks falling into this category include denial of service attacks, attempts to breach a firewall, and attempts to breach a router. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, involve attempts to make a computer resource unavailable to its intended users. Commonly, these attacks involve simply saturating the target machine with external internet requests. One of the most critical characteristics of cloud computing is its elasticity due to the

Table 6
Controls and countermeasures deployed through the adoption of cloud computing architecture, which attempt to counter previously identified threats.

		Characteristics of cloud computing architecture																
		Centralization/unified security architecture							Economies of scale	Location independence	Open free software/ centralization	Reliability						
		AC: access control, IA: identification and authentication, SC: systems and communications protection, AU: audit and accountability, CP: contingency planning							CP: contingency planning		AU: audit and accountability	CP: contingency planning						
		On-demand user security controls	Controlled execution environment	Encryption at rest and transit	Perimeter security (IDS, firewall, one time authentications)	Hypervisor protection against network attacks	Real-time detection of system tampering	Advanced honeynet capabilities	Low-cost disaster recovery and data storage solutions	Provision of data zones (e.g., by country)	Disclosability/ transparency	Data fragmentation and dispersal	Fault tolerance and reliability	Rapid re-constitution of services	Automated replication	VLAN capabilities		
Identified Treats e-Voting	Hardware modification								x		x		x	x				
	Hardware substitution								x		x		x	x				
	Hardware interception								x		x		x	x				
	Software modification																	
	• Trapdoors	x	x		x		x		x		x	x	x	x	x			
	• EasterEggs	x	x		x		x		x		x	x	x	x	x			
	• Logic bombs	x	x		x		x		x		x	x	x	x	x			
	• Information leaks	x	x		x		x		x		x	x	x	x	x			
	• Virus	x	x		x		x		x		x	x	x	x	x			
	• Trojan horse	x	x		x		x		x		x	x	x	x	x			
	Software deletion	x	x		x		x		x		x	x	x	x	x			
	Software theft	x	x	x	x		x		x		x	x	x	x	x			
	Malicious code on client	x	x		x				x		x	x	x					
	Man in the middle—*Replay*			x	x													
	Impersonation/ spoofing			x	x						x							
	Falsification of messages			x	x		x				x							
	DNS attack			x	x	x				x	x		x					x
	DDOS			x	x	x				x	x		x					x
	Connection flooding				x	x		x		x								x
	Traffic redirection			x							x							
	Session hijacking			x														
	Eavesdropping			x	x		x	x										x
	Wiretapping			x			x	x			x							x
	Misdelivery			x			x											
	Exposure within network			x	x	x	x				x							x
	Traffic flow analysis			x	x	x	x	x										

virtualization of servers. Information systems using a cloud computing infrastructure are able to respond to peaks in traffic with the creation of additional virtual servers. Elasticity, in combination with network filtering techniques available through a uniform security solution, can provide an effective and efficient response to network attacks such as DDoS. Network intrusion detection systems can provide adequate protection on the "systems perimeter".

Digital signatures and blind signatures based on PKI infrastructure allow for a horizontal infrastructure for both authentication and integrity features. PKI and encryption applications can make use of the cloud feature of the architecture, to provide hybrid solutions, enhanced by back-end security modules such as Hardware Security Module (HSM) devices. As a whole, PKI infrastructures and cryptography can benefit significantly from the cloud architecture, as an abstraction now exists between local security devices and network devices. Public key encryption is used to encrypt data in transit, ephemeral data on virtual instances, data storages, and network traffic.

The Serve security report (Jefferson et al., 2004, 2007) summarized a number of specific threats to electronic voting systems and points out the inefficiency of traditional architecture countermeasures to control these. In the following table the threats identified are weighed against the controls imposed by a cloud computing infrastructure.

A Cloud computing approach, complemented by several cryptographic technologies and supplementary controls, can assist in reducing previously identified threats and vulnerabilities (Table 7).

5. Assessment and future development

The cloud computing model offers a number of benefits, security and operational related, economic and business drivers, as opposed to traditional models. Leveraging existing IT infrastructure by adopting a cloud model, achieves a number of goals identified by initiatives and global regulations. e-Governments succeed in implementing a totally integrated presence, which has the ability to cross departments and layers of government, thereby increasing effectiveness and efficiency of services provided. In addition, organizational processes are improved while promoting a sustainable low carbon economy. Enabling secure electronic voting reinforces electronic democracy, as it targets at increasing deliberation in a bottom up method. It also increases efficiency and effectiveness of the electoral process and provides a macroeconomic, cost-efficient method for increasing election accuracy. In addition to increasing usability and accessibility, these Information Systems also aim at increasing transparency and openness in democracy. By providing more inclusive services, the social, geographical, and digital barriers experienced by numerous citizens are reduced.

As cloud computing is still in an embryonic stage, a number of identified challenges must still be overcome in order for it to succeed in the long run. These include the following:

- Legal complications of global data fragmentation. As data spans across diverse geographical locations and physical borders, legal barriers present themselves. Privacy and security has to be safeguarded with a regulatory legal framework. The cloud model, raises serious jurisdiction issues.
- Political issues. The cloud spans many borders and may be the ultimate form of globalization. Specific political groups may oppose this model.
- Security of virtual OSs in the cloud.
- Issues of cryptography.

Cloud computing has emerged as one of the most promising innovations of recent times in the field of information technology, with many advantages over traditional methods and models. In the long run, cloud computing's ability to overcome the previously identified challenges will define its acceptance and success.

6. Conclusion

In the future, cloud computing will inevitably support a surplus of information systems, as the benefits, specifically in the field of Information and Communication security, outnumber its shortcomings. Cloud computing offers a deployment architecture, which has the ability to address a number of vulnerabilities recognized in traditional IS. Cost effectiveness, geographical location independence, scalability, reliability, elasticity, and security are crucial aspects to the success of any information system, particularly e-Government. By reaping these benefits, e-Government can target a broader audience with a more inclusive, effective, and efficient platform. e-Voting is an element of electronic democracy which has previously fuelled concerns about privacy and security. It is becoming clear that electronic voting systems can enhance trust, as today's voting processes lack transparency and audit ability. As Information Systems and Communication Technologies are silently being integrated into different stages of the electoral process globally, it has become a necessity that we explore methods that enable *secure* electronic voting, while researching controls with the ability to reduce threats. The basic question in electoral administration no longer focuses on

Table 7
A Cloud computing approach, complemented by several cryptographic technologies and supplementary controls, can assist in reducing previously identified threats and vulnerabilities.

Threat	Traditional architecture countermeasures	Cloud architecture proposed solution controls
Trojan horse attack on PC to prevent voting	Can mitigate risk with careful control of PC software; reason for failure may never be diagnosed	Contained environment/software modifications disabled/client security applications/HIDS/auditability
On screen electioneering	Voter can do nothing to prevent this; requires new law	On screen electioneering can be prevented by making it technically infeasible to gain access onto the voter's terminal Disabled though desktop as a service, only encrypted communications permitted
Spoofing of system (various kinds)	None exist; likely to go undetected; launchable by anyone in the world	Encryption/authentication/digital signatures/perimeter security/client desktop is within security perimeter
Client tampering	None exist for all possible mechanisms. Too difficult to anticipate all attacks; most likely never diagnosed	Client environment centrally protected monitored/contained/within security perimeter/auditability
Insider attack on system servers	None within SERVE architecture; voter verified ballots needed; likely undetected	Transparency, openness, data fragmentation and dispersal, cryptography
System-specific virus	Virus checking software can catch known viruses, but not new ones; likely to go undetected	Real time detection of system tampering/on demand user security controls
Trojan horse attack on PC to change votes or spy on them	Can mitigate risk with careful control of PC software; harder to control at cybercafe, or other institutionally managed networks; attack likely to go undetected	Real time detection of system tampering/client environment centrally protected monitored/contained/within security perimeter/auditability
DDOS	Network filtering	Elasticity in combination with network filtering techniques, management layer is able to monitor traffic 24/7, centralized approach

whether ICT should be accepted in the electoral process, but rather on what kind of technology should be implemented, to what extent and what protection mechanisms should be applied. A combination of cloud computing and cryptography can address a number of the identified threats in cloud computing (i.e. integrity, confidentiality, authenticity, and availability of data and communications), effectively enabling secure electronic voting. Electronic voting can greatly benefit from the cloud computing model and hybrid architecture. The proposed e-Citizen cloud system includes the following identified characteristics:

- Centralization of security that would provide a uniform and consistent way to manage risk.
- Adoption of a common security foundation throughout the federal institutions and citizens information systems.
- Government-owned private cloud infrastructure offering desktop as SaS and a plethora of other tools including, email, security tools, etc.
- Encrypted access to service using PKI-based cryptography.
- Encryption of data at rest and in flight to the clouds.
- Data replicated over the clouds (on and off clouds) and across availability zones for data redundancy.
- Network intrusion detection on the system perimeter and real time detection of system tampering, (centralized Host Intrusion Detection Systems), providing a single access point based on PKI to all e-Government services.
- Centrally maintained and monitored, updates rolled out uniformly.

This paper investigated the advantages and disadvantages of adopting a cloud solution for electronic government deployed information systems. Following a thorough analysis of electronic voting security issues and vulnerabilities, the countermeasures offered by the adoption of a cloud architecture were reported. A proposed hybrid solution of electronic voting, making use of the described architecture, overcomes a number of IS security issues and has the capacity to reestablish trust in all Government election processes. It is crucial that further research is conducted in the field of electronic voting security, through official trials and pilots, before any solution is adopted for binding elections, as the integrity of the electoral system is at stake.

References

Bekkers, V. J., & Zouridis, S. (1999). Electronic service delivery in public administration: Some trends and issues. *International Review of Administrative Sciences*, *65*(2), 183−196, doi:10.1177/0020852399652004.

Buchsbaum, T. M. (2004). E-voting: International developments and lessons learnt. *Electronic Voting in Europe Technology, Law, Politics and Society*, 31−34.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. *Computing Research Repository - CORR*, 5−13.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599−616.

Capgemini (2009). 8th benchmark measurement, November 2009. *European Commission, Directorate General For Information Society And Media*.

Clive Sanford, J. R. (2007, Decemberr). Characterizing e-participation. *International Journal of Information Management*, *27*(6), 406−421.

Council of Europe, Committee of Ministers (2004). Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.

Cranor, L. (2003). In search of the perfect voting technology: No easy answers. In D. A. Gritzalis (Ed.), *Secure electronic voting: Advances in information security* (pp. 17−30). Norwell, MA: Kluwer Academic Publishers.

Deutsch, K. W. (1963). *The nerves of government: Mode/s of political communication and control.* New York: Free Press.

DiCaterino, A., & Pardo, T. A. (1996). The World Wide Web as a universal interface to government services. E-Government Act of 2002. Retrieved May 10, 2003, from,. http://www.ctg.albany.edu/resources/abstract/itt96-2.html.

EU Ministerial Declaration on e-Government. (2009). Malmö, Sweden.

Fuchs, C., Bernhaupt, R., Hartwig, C., Kramer, M. A., & Maier, U. (2006). *Broadening eParticipation: Rethinking ICTs and participation.* Internet Research 7.0. Brisbane, Australia: Association of Internet Researchers.

Ghere, R. K., & Young, B. A. (1998). The cyber-management environment: Where technology and ingenuity meet public purpose and accountability. *Public Administration and Management: An Interactive Journal*, *3*(1) Retrieved December 1, 2010 from:. http://www.pamij.com/gypaper.html.

Gritzalis, D. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539−556.

Heeks, R. (1998). Information systems and public sector accountability. The University of Manchester, Institute for Development, Policy and Management Information, Systems, Technology and Government: Working Papers Series, Number 1/1998.

Heeks, R. (1999). Information technology, government and development: Workshop report.

Heeks, R. (2001a). *Building e-governance for development: A framework for national and donor action.*The University of Manchester, Institute for Development, policy and management information, systems, technology and government: Working papers series Retrieved December 15, 2010 from. http://www.man.ac.uk/idpm/idpm_dp.htm#ig.

Heeks, R. (2001b). *Understanding e-governance for development.* The University of Manchester, Institute for Development, policy and management information, systems, technology and government: Working papers series, number 11/2001.

IBM (2009). *Seeding the clouds: Key infrastructure elements for cloud computing.*: IBM Retrieved December 1, 2010, from. http://www-35.ibm.com/services/in/cio/pdf/oiw03022usen.pdf.

Jaeger, P. T. (2003). The endless wire: E-Government as a global phenomenon. *Government Information Quarterly*, *20*(4), 323−331.

Jefferson, D., Rubin, A. D., & Simons, B. (2007). A comment on the May 2007 DoD report on voting technologies for UOCAVA citizens. Retrieved December 1, 2010, from. http://www.servesecurityreport.org/SERVE_Jr_v5.3.pdf.

Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004). A security analysis of the secure electronic registration and voting experiment (SERVE). Retrieved December 1, 2010, from. http://www.servesecurityreport.org/paper.pdf.

La Porte, T. M., De Jong, M., & Demchak, C. C. (1999). Public organizations on the World Wide Web: Empirical correlates of administrative openness. Retrieved December 1, 2010, from. http://www.cyprg.arizona.edu/publications/correlat.rtf.

McClure, C. R., & Bertot, J. C. (2000). The Chief Information Officer (CIO): Assessing its impact. *Government Information Quarterly*, *17*(1), 7−12.

McGregor, E. B., Jr. (2001). *Web page accountability: The case of public schools.* Bloomington, IN: Paper presented at the National Public Management Research Conference.

Memorandum for chief information officers (2007). *Planning guidance for Trusted Internet Connections (TIC).* Washington, United States..

MIT (2001). *Voting: What is, what could be, report of the CalTech MIT Voting Technology Project.*

Mohen, J., & Glidden, J. (2001). The case for internet voting. *Communications of the ACM*, *44*(1), 72−85.

Montagna, J. M. (2005). A framework for the assessment and analysis of electronic government proposals. *Electronic Commerce Research and Applications*, *4*(3), 204−219.

Naone, E. (2009). Technology overview: Conjuring clouds. MIT Technology Review, July/August. Retrieved December 15, 2010, from. http://www.technologyreview.com/computing/22606/?a=f.

National Institute of Standards and Technology (NIST) (2009). US Federal Cloud Computing Initiative RFQ (GSA). U.S. government.

NISp, & Peter Mell, T. G. (2009). *The NIST definition of cloud computing.* National Institute of Standards and Technology, Information Technology Laboratory.

NIST Draft SP 800-39 (2008). *Managing risk from information systems: An organization perspective.* National Institute of Standards and Technology.

NIST Draft SP 800-53 (2007). *Recommended Security Controls for Federal Information Systems and Organizations*: National Institute of Standards and Technology.

NIST SP 800-53 (2008). *Recommended security controls for federal information systems.* National Institute of Standards and Technology.

NIST SP 800-53A (2008). *Guide for assessing the security controls in federal information systems.* National Institute of Standards and Technology.

NIST SP 800-59 (2003). *Guideline for identifying an information system as a national security system.* National Institute of Standards and Technology.

NIST Special Publication 800-60 (2008). *Guide for mapping types of information and information systems to security categories. Volume I.* National Institute of Standards and Technology.

NIST SP 800-46 (2009). *Guide to enterprise telework and remote access security*. National Institute of Standards and Technology.

Open Government Iniative (2009). *Memorandum for the heads of executive departments and agencies, Washington, US.* .

Parycek, P. S. (2003). *Electronic democracy: Chances and risks for municipalities.* E-Democracy: Technology, right and politics. Vienna: OCG.

Peter Mell, T. G. (2009). *Effectively and securely using the cloud computing paradigm.* : NIST, Information Technology Laboratory.

Pfleeger, C., & Pfleeger, S. (2006). *Security in computing.* Upper Saddle River, NJ: Prentice Hall.

Reese, G. (2009). *Cloud application architectures: Building applications and infrastructure in the cloud.* Sebastopol, CA: O'Reilly Media.

Riera, A., & Brown, A. R. (2003). Bringing confidence to electronic voting. *Electronic Journal of e-Government*, *1*(1), 1−64.

Sun Microsystems (2009). Introduction to cloud computing architecture. White paper. Retrieved from,. http://webobjects.cdw.com/webobjects/media/pdf/Sun_Cloud-Computing.pdf.

U.S. Federal Cloud Computing Initiative (July 30, 2009). Retrieved December 1, 2010, from. http://www.scribd.com/doc/17914883/US-Federal-Cloud-Computing-Initiative-RFQ-GSA.

U.S. Public Law 107 - 347 - E-Government Act of 2002, H.R. 2458, December 17, 2002.

UN&ASPA—United Nations/American Society for Public Administration (2002). Benchmarking e-Government: A global perspective. http://unpan1.un.org/intra-doc/groups/public/documents/un/unpan021547.pdf.
Verdegem, P., & Verleye, G. (2009). User-centered e-Government in practice: A comprehensive model for measuring user satisfaction. *Government Information Quarterly*, *26*(3), 487—497.
Von Lucke, J., & Reinermann, H. (2004). Definition of electronic government. Retrieved December 1, 2010, from. http://foev.dhv-speyer.de/ruvii.
Wardley, S., Goyer, E., & Barcet, N. (2009). *Ubuntu Enterprise Cloud Architecture*. Technical White Paper. Canonical.
Williams, B. J. (2004). Implementing voting systems — The Georgia method. *Communications of the ACM*, *47*(10), 39—42.
Wimmer, M. A. (2002). Integrated service modeling for online one-stop government. *Electronic Markets*, *12*(3), 149—156.
Wolfram Alpha (2009). Wolfram alpha. Retrieved November 4, 2009, from Wolfram Alpha. http://www.wolframalpha.com/input/?i=internet+users.
Xenakis, A. (2004). Procedural security in electronic voting. *37th Hawaii International Conference on System Sciences*.
Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, *24*(3), 646—665.

Dimitris Zissis holds a BSc in Computer Science, an MSc in Computing and Information Systems, and an MBA in General Management; he is currently pursuing a PhD in Information and Communication Security at the University of the Aegean in Greece. He has been involved in a number of EU funded research projects, mostly in the research area of IT Security, involving the development of e-Governance solutions and deploying public key infrastructures cryptography.

Assistant Professor Dimitrios Lekkas holds a Ph.D. in the area of Information Systems Security, an MSc in Information Technology and a BSc in Mathematics. He is a lecturer at the Department of Product and Systems Design Engineering of the University of the Aegean, Greece. He has participated in many research projects funded nationally and by the European Union and published several papers in international journals and presented several papers at conferences. He is a member of the Greek National Educational Network (EDUnet) technical committee and coordinator of the e-School and the e-University Public Key Infrastructure (PKI). His current research interests include design of information infrastructures, computer security, incident response, public key cryptography and digital signatures, and database management systems.