Chapter 92
Security and Privacy Issues in Cloud-Based E-Government

Heru Susanto
Universiti Brunei Darussalam, Brunei & The Indonesian Institute of Science, Indonesia

Mohammad Nabil Almunawar
Universiti Brunei Darussalam, Brunei

ABSTRACT

Cloud computing services have grown rapidly over the years. Government agencies are also interested in cloud-based provision for their E-government processes. Despite the advantages of cloud-related technologies, there are many security issues as well that fall into several categories of breaches with serious impacts. All these breaches have serious legal and reputational implications. Therefore, governments need to ensure that inherent security threats can be neutralized to ensure that data or information stored in the cloud are well protected. It is imperative for cloud-based e-government (CB-eGov) to use an information security management system (ISMS) to effectively manage CB-eGov. The purpose of this chapter is to discuss how cloud computing can be incorporated in an e-government implementation to improve its efficiency without compromising information security. As such, the government needs to take special care in ensuring security, privacy, and confidentiality of information stored in the cloud.

INTRODUCTION

Information security is important in any information system. It becomes crucial if the system is accessible through a computer network, especially a public network such as the Internet. Most e-government systems nowadays are accessible through the Internet; hence, their existence is highly influenced by their securities. If an e-government system is attacked, say, by website defacement, it will create many problems, including downgrading of the credibility of the entire e-government system. As a result, the users (citizens and the business sector) will hesitate to use the system as they lose their trust in the system and then the transactions using the system will suffer. One example of a security attack is denial of service (DoS), which can make a system inaccessible through the Internet.

DOI: 10.4018/978-1-5225-8176-5.ch092

Before we discuss security issues in e-government, especially cloud-based e-government, here is what we mean by e-government. An e-government system can be seen as a concept of using information and communication technology (ICT) to not only organize and manage information but also facilitate administrative processes in government, transactional and interactive processes between government and public. In general, an e-government system has two main subsystems, the front-end system that interacts with users and the back-end system that performs all necessary processes to fulfil requests from the users through the front-end system (Lambrinoudakis et al., 2003). The back-end system is normally composed of web server(s), database server(s) and other necessary software. The back-end system normally resides on government premises, managed and maintained by the government. The front-end systems are users' devices (desktops, laptops, tablets, and smart phones) equipped with client programs that can access the back-end system through the Internet.

The government can outsource the back-end system to a cloud provider, creating a cloud-based e-government system (CB-eGov). As servers and related software are outsourced to a cloud provider, the problem of server maintenance and software update can be avoided. Cloud-based e-government (CB-eGov) is an interesting idea as it can provide quality service delivery to the public with many benefits compared to the old way. Cloud computing is flexible, scalable and relatively inexpensive as compared to the conventional approach of computing (Chen & Almunawar, 2015). However, despite many benefits offered by cloud computing in implementing e-government, there are security issues and risks that need to be understood and addressed properly. In fact, one of the main obstacles to adoption of cloud computing for e-government is the perception of lost control as the back-end system no longer resides in a location under the government control. This perception creates hesitancy concerning the security of CB-eGov.

Numerous possible security breaches can happen in any CB-eGov. In general, security breaches associated with CB-eGov or any information system can be divided into three categories. Firstly, breaches with serious criminal intent (fraud, theft of commercially sensitive or financial information). Secondly, breaches caused by 'casual hackers' (defacement of web sites or 'denial of service' which cause web sites to crash). Thirdly, the flaws in systems design and/or set up leading to security breaches (genuine users seeing/being able to transact on other users' accounts). All of these threats have serious potential for legal and reputations implications. All possible security breaches need to be addressed comprehensively and systematically as security involves both technical and non-technical aspects. An information security standard can be adopted to address all possible security issues. A compliance to an information security standard can help to boost confidence on security of an information system, including CB-eGov.

This chapter is organized as follows. The following section discusses CB-eGov. The next section discusses information security awareness within CB-eGov, followed by a discussion on potential security attack on CB-eGov. In order to protect information system resources, this chapter also looks at several information systems security standards and provides a comparison between them. Next, we discuss potential security attacks in CB-eGov followed by a discussion on how to monitor such attacks. The chapter ends with a conclusion making recommendations for future research directions.

UTILIZING CLOUD COMPUTING FOR E-GOVERNMENT

Cloud computing is a computing model where the computing resources are provided by cloud providers and used by the consumers on demand. The National Institute of Standards and Technology (NIST)