Chapter 11
Data Security for Connected Governments and Organisations:
Managing Automation and Artificial Intelligence

Heru Susanto
https://orcid.org/0000-0002-1823-357X
The Indonesian Institute of Sciences, Indonesia & Brunei University of Technology, Indonesia

Leu Fang Yie
Computer Science Department, Tunghai University, Taiwan

Didi Rosiyadi
The Indonesian Institute of Sciences, Indonesia

Akbari Indra Basuki
The Indonesian Institute of Sciences, Indonesia

Desi Setiana
Universiti Brunei Darussalam, Brunei

ABSTRACT

Digital ecosystems have grown rapidly over the years, and governments are investing in digital provision for their processes and services. Despite the advantages of distributed technologies, there are many security issues as well that result in breaches of data privacy with serious impact including legal and reputational implications. To deal with such threats, government agencies need to thoughtfully improve their security defences to protect data and systems by using automation and artificial intelligence (AI), as well as easing the data security measures including early warning of threats and detection. This study provides a comprehensive view of AI and automaton to highlight challenges and issues concerning data security and suggests steps to combat the issues. The authors demonstrate the role of AI-driven security tools and automation to mitigate the impact of data breaches to also propose recommendations for government agencies to enhance their data security protection.

DOI: 10.4018/978-1-6684-3694-3.ch011

INTRODUCTION

In a multi-platform technological environment, with the convenience of cloud-based services and a fully realized mobile workforce, data may not be as safe and, therefore, may not be completely under our control. Data are constantly at risk of being accessed by unauthorized personnel and shared with other unauthorized people. Since, information security is important in any information system, security becomes crucial if the system is accessible through a computer network, especially a public network such as the Internet. Since, most governmental business processes are digitally based systems accessible through the Internet, their existence and functionality are highly influenced by the level of in-built security. In fact, a digital connected government has a much broader scope of electronic government, as it refers to and deals with smarter environments e.g. smart city, smart health, smart transport, documents citizenship, citizen subsidies, etc. If a digital 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 systems as they lose their trust in them, and then the transactions made through the systems will suffer.

With the above background, digital governments need to divert their attention to identifying sensitive data and develop their data security strategy away from the traditional network-centric view to focus more on data-centric aspects. Data-centric approach to security can be exploited to let business processes to focus on the sensitive data to be protected. Data centric security can be defined as an approach to security that has emphasis on securing sensitive data itself rather than the security of networks, servers or applications. The common prevention mechanisms of firewalls and access controls may be helpful at times but these will not necessarily be able to protect the data stored in the cloud environment or shared via emails. Protecting sensitive information in the files can take advantage of the cloud computing paradigm, mobile related technologies and other innovations without placing the businesses at risk (Leu et al., 2015; Liu et al., 2018).

In general, digital government systems comprise two main subsystems: the front-end component that interacts with users, and the back-end component that performs all necessary processes to fulfil requests from the users through the front-end component. The back-end system is normally composed of web servers, database servers and other necessary software. It normally resides within government premises, managed and maintained by the government departments. The front-end system refers to user devices (e.g. desktops, laptops, tablets, and smart phones) equipped with client related programs (such as applications to consume e-services) that can access the back-end system via the Internet. The government can outsource the back-end system to third parties such as a cloud provider, in which case, creating a cloud-based digital government system (CB-dGov). As government servers and related software are often outsourced to cloud providers, the problem of server maintenance and software update can be avoided, as it becomes the responsibility of the cloud providers.

The cloud-based digital government system (CB-dGov) is an interesting idea as it can provide quality service delivery to the public with many benefits compared to the old ways. Cloud computing is flexible, scalable and relatively inexpensive as compared to the conventional approach of computing. However, despite many benefits offered by cloud computing in implementing CB-dGov, there are security issues and risks that need to be understood and addressed properly. In general, security breaches associated with CB-dGov or any information system can be divided into three categories: