Chapter 20
Configuring a Trusted Cloud Service Model for Smart City Exploration Using Hybrid Intelligence

Manash Sarkar
Birla Institute of Technology, Mesra, India

Soumya Banerjee
Birla Institute of Technology, Mesra, India

Youakim Badr
National Institute of Applied Sciences of Lyon, France

Arun Kumar Sangaiah
VIT University, India

ABSTRACT

Emerging research concerns about the authenticated cloud service with high performance of security and assuring trust for distributed clients in a smart city. Cloud services are deployed by the third-party or web-based service providers. Thus, security and trust would be considered for every layer of cloud architecture. The principle objective of cloud service providers is to deliver better services with assurance of trust about clients' information. Cloud's users recurrently face different security challenges about the use of sharable resources. It is really difficult for Cloud Service Provider for adapting varieties of security policies to sustain their enterprises' goodwill. To make an optimistic decision that would be better suitable to provide a trusted cloud service for users' in smart city. Statistical method known as Multivariate Normal Distribution is used to select different attributes of different security entities for developing the proposed model. Finally, fuzzy multi objective decision making and Bio-Inspired Bat algorithm are applied to achieve the objective.

DOI: 10.4018/978-1-5225-5634-3.ch020

INTRODUCTION

Smart city, a standard planed city, encompasses variety of network services for enterprise and individuals. The services are provided by different kind of domain specific vendors, which lead to limited *scalability and extensibility.* Recently, smart-city services are typically provided in single domains like Internet service, building management, transportation, and health care. Recent trend of service provider is to provide service based on on-demand process. The concept of cloud computing is implemented for using virtualized on-demand network services. Therefore, cloud computing becomes popular to internet users in context of smart city. Basically, cloud computing is applicable in different Government, public and private sectors. People, from last few years, downloaded different software to run applications or programs in their computer or server. People use online social networks to maintain their social community, avail different kinds of online banking transaction and also access variety of online application to make their video chatting for communication regularly through internet. Cloud computing provides same kinds of applications through internet based on clients' demand. Therefore, cloud based services are ideal for not only business organizations but also beneficial for individuals in concept of smart city (Chourabi et al. 2012; Clohessy et al. 2014). Present era heartily welcomes the concept of cloud computing for trending the smart city. Therefore, security and privacy of cloud computing are crucial issues to maintain the trust in a smart city. The responsibility of CSP is to guarantee the people of smart city that their information is in safe (Ferraz et al. 2014; Solankia et al. 2016). In a smart city, CSP are responsible to ensure secured communication between authorized users' and provides secured data exchange in multimedia system (Dey & Santhi 2017). Improvement of efficient and trusted on-demand services have been enhanced dramatically through proper utilization of centralized resources.

Therefore, the concept of trusted cloud computing has been introduced. It is mandatory to maintain trust between every entity within same context for building a trusted environment (Sarkar et al. 2015). In case of secured smart city, trust would be maintained between every user. The flexibility and cost effectiveness of cloud computing made an arena for servicing consumers' and enterprises' requirements. The popularity and flexibility of cloud computing sometime become threat for itself. Thus, security and privacy are crucial issues for cloud architecture (Ranabahu et al. 2009; NIST Special Publication 2011). The basic idea of security in cloud computing follows the context of cloud infrastructure (Ahmed & Hossain, 2014). The study of security, privacy and trust in cloud environment enhances the knowledge about different kind of threats and their countermeasures (Khalil et al. 2014). It is a responsibility for CSP to deploy different security issues according to cloud environment and varieties of cloud services. Security issues and risks of cloud environment were also discussed by Pingree (Khalil, 2010). The author described that the potential risks of all cloud system was enhanced by the issue of violation for virtualization software. To sustain the goodwill of third party service provider, different types of optimistic decision would be initiated. Different cloud service providers use different types of security policies for their business model. Microsoft offers cloud services such as Windows Azure, Business Productivity Online Standard Suite (BPOS) and Windows SkyDrive (Microsoft Azure, 2016). Amazon another company handles customer relations based on their feedback. EC2 (Amazon Elastic Compute Cloud) (Amazon web services, 2016) is a simple web based service interface allows clients to obtain and configure capacity with minimal friction. Amazon web service (AWS) provides storage, database, broad set of global compute, analytics, application and deployment services for business and public organizations to move faster, less IT costs.