Chapter 6
Privacy in Cloud-Based Computing

Monjur Ahmed
https://orcid.org/0000-0003-1929-3950
Waikato Institute of Technology, New Zealand

Nurul I. Sarkar
https://orcid.org/0000-0003-2770-8319
Auckland University of Technology, New Zealand

ABSTRACT

Cloud computing, internet of things (IoT), edge computing, and fog computing are gaining attention as emerging research topics and computing approaches in recent years. These computing approaches are rather conceptual and contextual strategies rather than being computing technologies themselves, and in practice, they often overlap. For example, an IoT architecture may incorporate cloud computing and fog computing. Cloud computing is a significant concept in contemporary computing and being adopted in almost every means of computing. All computing architectures incorporating cloud computing are termed as cloud-based computing (CbC) in general. However, cloud computing itself is the basis of CbC because it significantly depends on resources that are remote, and the remote resources are often under third-party ownership where the privacy of sensitive data is a big concern. This chapter investigates various privacy issues associated with CbC. The data privacy issues and possible solutions within the context of cloud computing, IoT, edge computing, and fog computing are also explored.

INTRODUCTION

The emergence of few recent computing approaches bring new paradigm to computing world. Examples of such computing approaches are Cloud Computing, IoT, Edge Computing and Fog Computing. With numerous benefits and advantageous features, all these computing approaches come with a severe downside – that is, security. Security is a major concern for the above computing approaches from perspectives

DOI: 10.4018/978-1-7998-8954-0.ch006

of business strategy as well as technological and Human Factors. These computing approaches use and/or transfer an organisation's digital assets (i.e., digital information) off-site for various purposes.

Cloud Computing, IoT, Edge Computing and Fog Computing have become a hype. Organisations are submerging themselves in this hype and – in some cases, discussed later in this chapter– handing over digital assets to third parties. Using computing techniques like Cloud Computing may incorporate moving data into remote computers that are geographically dispersed and crossing political geographic boundaries. Besides, the aforementioned computing techniques use latest technologies, computing devices and gadgets (e.g., smart phone). Electronic end-user gadgets, when become part of a network as an end-user terminal or node, may pose security and privacy concerns. The infrastructural settings of recent computing approaches in terms of location of various elements (e.g., computers, data storage, processing) are crucial factors in information security and privacy. Based on the locations of architectural/infrastructural elements, Cloud Computing, Fog Computing and Edge Computing may introduce a very complex scenario for organisations in terms of Governance, Risk and Compliance (GRC).

Cloud Computing incorporates numerous security concerns (Ahmed & Hossain, 2014; Ahmed, Litchfield & Ahmed, 2014; Ahmed & Litchfield, 2016; Khalil, Khreishah & Azeem, 2014; Aljawarneh & Yassein, 2016; Kar & Mishra, 2016). From an information security and privacy viewpoint, this chapter investigates the computing techniques that use Cloud Computing. Cloud Computing, Fog Computing, Edge Computing, IoT – these are few recent computing techniques/approaches considered in this chapter.

All kinds of CbC uses remote resources and infrastructure that are owned and managed by third party vendors. This results in a situation where customers (individual or organisation) hand over their data to the vendors. Customers' data and information reside in the vendors infrastructures and servers dispersed geographically around the globe. This results in various complex scenario that are considered as threat to information privacy and security in cyber space. The focal point in this chapter is how CbC may have an impact on the privacy of an organisation's digital assets.

Cloud, Fog, Edge Computing, and IoT

Location of the users as well as the computing and networking devices & elements, and the types of devices used in a computing setting are significant contributing factors in information privacy and security. This section presents the concept of Cloud Computing, Fog Computing, Edge Computing and IoT, with a focus on the locations of various infrastructural elements involved in these computing settings.

Cloud Computing means using remote computing resources or infrastructure for computing and/or data storage purposes (Ali & Haseebuddin, 2015; Birje, Challagidad, Goudar & Tapale, 2017; Cardoso & Simões, 2011; Jadeja & Modi, 2012). Such remote computing infrastructures are normally 'borrowed' or 'rented'. The provider and owner of such infrastructures are third parties known as Cloud Service Provider (CSP). The end-users (individuals or organisations) utilise the CSPs computers (i.e., Cloud servers) or infrastructure to store data or for computing purposes. Figure 1 illustrates the concept of Cloud Computing.

When it comes to IoT, an infrastructure implementing IoT may incorporate Cloud Computing, Fog Computing and Edge Computing. To explain this, Figure 4 portrays the conceptual architecture and the core layers of an IoT infrastructure.