

Chapter 9

Solutions for Securing End User Data over the Cloud Deployed Applications

Akashdeep Bhardwaj

University of Petroleum and Energy Studies (UPES), India

ABSTRACT

With more and more organizations working on the cloud over unsecure internet, sharing files and emails and saving them on cloud storage imperative. Securing the end user sensitive data in transit has thus started to get maximum priority to protect it from Cloud company staff, hackers and data thieves. In this study, an attempt is made to review the research of end user data security. There is an urgent need for solutions for end users' data protection, privacy and during the times when migrating from one Cloud service provider to other. This chapter identifies end user data challenges and issues on cloud and presents use of Public Key Cryptography, Multi Factor Authentication and use of Cloud Aware applications as possible solutions.

DOI: 10.4018/978-1-5225-1941-6.ch009

Copyright ©2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION TO END USER COMPUTING

Cloud based services provide flexible, scalable, pay-per-use, short term contract model for the IT Services make Cloud based services an efficient, affordable and easy to implement option reducing capital expenditure involving IT hardware, licenses, office space, computing power and bandwidth. Security of user data needs to be in place more so in today's context with Cloud based application being hosted on the service provider premise as well as the end user residing in a remote data center, well outside the user's control.

As per a recent survey conducted by International Data Group (IDG), the top three challenges for implementing cloud based security strategy differs between IT and the line-of-business (LOB). A survey conducted by International Data Corporation (IDC) declares that 47% IT Heads are highly concerned about security threats in cloud computing. In a recent survey conducted by Cisco, two thirds of the respondents acknowledged that security and privacy are the top two security issues for cloud consumers. This chapter reviews the challenges in Cloud computing services regarding end user data, analyzing the issues face and presents solutions to overcome them (Schutz et al., 2016). The end user data required to be protected is of four types ranging from usage data which is the information collected from computer systems, then is the sensitive information on health and bank accounts, then is the Personally identifiable information; information to identify an individual and finally is the Unique device identity information that is uniquely traceable like IP addresses, unique hardware identities (MAC address). By using solution paths such as digital keys, multi factor authentication and cloud aware applications.

When there is a need to provide End users with the right type of IT resources to enable them to perform their tasks, usually we do not emphasize on importance of securing the end user data (Bouchana et al., 2015). End user data for end user functionalities such as support, buying hardware, software and licenses, then plan endlessly for installation, support, maintenance as well as worry about capacity planning, creating IDs, configuring profiles or sit on a budgeted pile of money waiting for hiring to be completed.

1. **Web Based Services:** Internet email services (Gmail, Yahoo, and Hotmail), Online stores (Amazon, Fab furnish, Jabong), Web hosting (NetMagic, Tulip). These have been around for many years.
2. **Distributed Computing:** Splitting the processing workload among multiple systems usually connected at the same sites like being done in Parallel and Grid computing technologies.
3. **Datacenters:** Single application being hosted in one location (over single or even multiple servers) does not qualify as a Cloud. Cloud computing lever-

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/solutions-for-securing-end-user-data-over-the-cloud-deployed-applications/173135

Related Content

Classification Based on Unsupervised Learning

Yu Wang (2009). *Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection* (pp. 348-395).

www.irma-international.org/chapter/classification-based-unsupervised-learning/29702

IoT an Efficient Privacy Preserving Scheme for Internet of Things Environment

Shelendra Kumar Jain and Nishtha Kesswani (2020). *International Journal of Information Security and Privacy* (pp. 116-142).

www.irma-international.org/article/iotp-an-efficient-privacy-preserving-scheme-for-internet-of-things-environment/247430

Use of Social Media for Women Entrepreneurship (With Special Reference to Bhopal)

Neel Rai and Rajeev Sijariya (2020). *International Journal of Risk and Contingency Management* (pp. 20-28).

www.irma-international.org/article/use-of-social-media-for-women-entrepreneurship-with-special-reference-to-bhopal/247141

Building an Online Security System with Web Services

Richard Yi Ren Wu and Mahesh Subramaniam (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1027-1047).

www.irma-international.org/chapter/building-online-security-system-web/23141

Content-Based Collaborative Filtering With Predictive Error Reduction-Based CNN Using IPU Model

Chakka S. V. V. S. N. Murty, G. P. Saradhi Varma and Chakravarthy A. S. N. (2022). *International Journal of Information Security and Privacy* (pp. 1-19).

www.irma-international.org/article/content-based-collaborative-filtering-with-predictive-error-reduction-based-cnn-using-ipu-model/308309