

Chapter 34

Evaluation of Reliable Data Storage in Cloud Using an Efficient Encryption Technique

Saswati Sarkar

Computer Innovative Research Society, India

Anirban Kundu

 <https://orcid.org/0000-0001-9615-4917>

Netaji Subhash Engineering College, India

Ayan Banerjee

Computer Innovative Research Society, India

ABSTRACT

Cloud-based reliable and protected data storage technique is proposed in this chapter. The proposed technique encrypts and protects data with less time consumption. Power consumption of storage is dependent upon capacity of storage and physical size of storage. Time analysis is presented graphically in this chapter. Reliable data storage is represented in cloud based proposed approach. Data is encrypted with minimum time complexity due to usage of proposed cloud-based reliable data storage. The competent ratio of time complexity is graphically observed in proposed data storage technique. Power consumption of storage has been typically dependent on the basis of capacity of storage and amount of storage. A ratio of power consumption and capacity of storage is presented in cloud-based approach. An efficient usage of energy is shown depending on current consumption and voltage in proposed reliable approach.

INTRODUCTION

Overview

Storage devices (as found in “<http://smallbusiness.chron.com/difference-between-25-35-hard-drives-67453.html>”) consist of computer hardware that is used for storing data which can hold and store information temporarily and permanently. Computer data storage is known as storage or memory (as found in “<https://www.quora.com/How-do-hard-drives-of-the-same-physical-size-vary-in-capacity-of-storage>”). Storage device is consisting of computer components used to retain digital data.

Storage devices are typically utilized in internet based hardware and software resources, information technology paradigm shift, and cloud computing (Daniel J. A., 2009). There are different types of cloud computing services are available today such as Amazon EC2, Google Apps, Apple iCloud etc.. There are two factors such as advanced software applications and high-end networks of server-side computer systems are required for maintaining the reliability of services (Aboroujilah A., Amusa A.S., 2017). There are several components such as development of grid computing, parallel computing, distributed computing, big data analysis (Alsghaier H., Akour M., Shehabat I., Aldiabat S., 2017), and utility computing have been incorporated in cloud computing (Agarwal H., Sharma A. 2016). Cloud based services have been extended in distinct fields such as virtual IT, software and network storage (Kandukuri B. R., Paturi R. V., Rakshit A., 2009).

Reliability is a attribute, which has been measured depending on consistent performance of different computer related component such as network, software, hardware (Subashini S., Kavitha V., 2011) (Zhang X., Wuwong N., Li H., and Zhang X. J., 2010). Mean Time to Data Loss (MTTDL) matrix is required to calculate reliability. The amount of expected elapse time has been described by this matrix until first data loss. There are two purposes such as encryption (IGI global, 2017) of backed-up data, and decryption of backed-up data have been resolved by using two-way function called encryption. Encryption (IGI Global, 2016) has been incorporated as a characteristics of storage security (Das D., Misra R., 2011). There are two different message formats such as plaintext and ciphertext have been required to perform encryption algorithm and decryption algorithm (Parsi K., Sudha S., 2012).

Power (as found in “<http://www.tomshardware.com/reviews/geforce-radeon-power,2122-7.html>”) is energy over time. The unit of power is watt. Power (Watts) is Joules per second.

Power (Watts) = E/T = Energy (Joules) / Time (Seconds).

Energy, $E = P \cdot T$, where P = Power, and T = Time.

A watt hour is a unit of Energy, an alternative to Joules (Pinheiro E., Bianchini R., Dubnicki C., 2006). Voltage is known as electromotive force which is a quantitative expression of the potential difference in charge between two points in an electrical field.

$P = IV$ (Power = Current * Voltage)

(<http://www.tomshardware.com/reviews/desktop-hdd.15-st4000dm000-4tb,3494-6.html>).

13 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/evaluation-of-reliable-data-storage-in-cloud-using-an-efficient-encryption-technique/280202

Related Content

Privacy and Banking in Australia

Supriya Singh (2009). *Handbook of Research on Social and Organizational Liabilities in Information Security* (pp. 161-174).

www.irma-international.org/chapter/privacy-banking-australia/21340

Protecting Patient Information in Outsourced Telehealth Services: Bolting on Security when it cannot be Baked in

Patricia Y. Loganand Debra Noles (2008). *International Journal of Information Security and Privacy* (pp. 55-70).

www.irma-international.org/article/protecting-patient-information-outsourced-telehealth/2487

Aligning Assurance Requirements, Countermeasures, and Business

Craig E. Kaucher (2004). *Information Technology Security: Advice from Experts* (pp. 14-40).

www.irma-international.org/chapter/aligning-assurance-requirements-countermeasures-business/24771

Hexa-Dimension Code of Practice for Data Privacy Protection

Wanbil William Lee (2019). *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics* (pp. 237-248).

www.irma-international.org/chapter/hexa-dimension-code-of-practice-for-data-privacy-protection/213654

On Access-Unrestricted Data Anonymity and Privacy Inference Disclosure Control

Zude Liand Xiaojun Ye (2008). *International Journal of Information Security and Privacy* (pp. 1-21).

www.irma-international.org/article/access-unrestricted-data-anonymity-privacy/2490