Chapter 4
Cloud Cryptography

Renuka Devi Saravanan
Vellore Institute of Technology, Chennai, India

Shyamala Loganathan
Vellore Institute of Technology, Chennai, India

Saraswathi Shunmuganathan
Sri Sivasubramaniya Nadar College of Engineering, Chennai, India

ABSTRACT

Cloud computing is a recent technology that facilitates wide access and storage on the internet. Cloud computing faces few challenges like data loss, quality issues, and data security. Data security became a major concern in the cloud domain as the demand for cloud services is increasing drastically due to its scalability and allowance of concurrent access to users for using various cloud resources. As a consequence, malicious attacks and data breaches happen which also affect other cloud users. Cloud security is made possible with cryptography, which protects from malware and unauthorized users. Traditional cryptographic algorithms are often used to provide data privacy, integrity, and confidentiality. Most recently, a new data encryption scheme was proposed for cloud computing that uses quantum cryptography to improve security. The proposed chapter will provide the complete details about need of data security in cloud computing, significance of cryptography in cloud, existing cryptographic solutions, and proposes a generic model for cloud data security.

INTRODUCTION

National Institute of Standards and Technology (NIST) proposed and described cloud computing, a new century-old technology, in 2006. The rise and development of cloud technology is unexpected in many ways, including cost, stability, performance, and storage capacity. The cloud computing environment allows storing and sharing a huge volume of digital data like text, image, audio, video, etc. through the Internet (Sahinoglu and Cueva-Parra, 2011). It has become an exclusive technology due to its flexibility to access the data at any time as per user convenience. Cloud computing capabilities are now necessary for practically all business types. Taking into account aspects like vast storage and cost-effectiveness,

DOI: 10.4018/979-8-3693-0900-1.ch004

the adoption of cloud-based environments and IaaS, PaaS, or SaaS computing models has increased in contemporary organizations((Mell and Grance, 2011). They provide data storage, facilitate real-time communication and collaboration, and connect new gadgets to business networks. Crucially, cloud installations may scale up fast, which has aided numerous businesses in creating new relationships and working environments with external teams, partners, clients, and remote workers.

However, due to its centralized storage, Cloud computing faces few challenges like data loss, quality issues, and data security. Data security became a major concern in the cloud domain as the demand for cloud services is increasing drastically due to its scalability and allowance of concurrent access to users for using various cloud resources. As a consequence, malicious attacks and data breaches happen which also affect other cloud users using the same resources within the organizations that use cloud services. A study found that 85% of business executives cited security as the biggest obstacle when it comes to cloud computing (IBM Data Breach Report, 2022). One issue is that a lot of businesses just haven't evaluated the risks involved with cloud deployments or figured out what security aspects are under their purview. It can be difficult to ascertain which components of these systems need to be maintained because the majority of businesses rely on cloud service providers, or CSPs. Cloud security should follow a "cover the basics" approach that includes fundamentals, such as: A thorough understanding of the data gathered, powerful identity and authentication tools, Access controls based on the principle of least access, Correct configuration of the deployment, encryption of data in motion, in use, at rest, network activity monitoring limited privileged access to cloud settings, proper training of IT, security and individual users(Chitturi and Swarnalatha, 2020).

A CSP may offer continuous monitoring solutions to help detect suspicious user activity and assess an organization's threat status in real time. The process of storing the data in the cloud securely is made possible with cryptography in the cloud which protects from malware and unauthorized users. Encryption technique is used for the security of the data hosted by cloud providers and limited users can access the services that were shared by cloud providers comfortably and securely. Cryptography provides integrity, confidentiality, and authentication and it mainly secures the information from unauthorised/ third-party access.

Rest of the chapter discusses the need of cloud security and the challenges involved in it, elaborates the different security techniques exist at present with their advantage and disadvantage, reviews the security services required in CSP and suitability of the existing techniques, proposes a model for cloud data security.

NEED FOR CLOUD SECURITY

Organizations can outsource many of the time-consuming IT-related duties thanks to these as-a-service models(Xiao et al., 2016). Technology and numerous other technology-related aspects have evolved over time with regard to how businesses operate digitally. Most businesses today take liberty of the advantages of digital data sharing and storage, which greatly facilitate and accelerate their work. Organizations of all sizes typically benefit from this form of data computing. It can significantly assist these firms in managing IT-related infrastructure while also assisting them in lowering their capital expenditures. It should also be noted that as technology has advanced, most businesses have switched to online forms and are creating larger, more effective digital infrastructure. It is crucial that businesses use strategies that other businesses use in platforms that are compatible with their own. The majority of businesses