Chapter 5
Secure Data Sharing Using Revocable-Storage Identity-Based Encryption

Muthumanikandan Vanamoorthy
Vellore Institute of Technology, Chennai, India

ABSTRACT

Distributed computing provides flexible and informative information exchange and brings many benefits to both the general public and individuals. However, because the information often contains the most important data, there is a common lock that allows users to easily reuse cloud host information. Therefore, it is important for users to provide cryptographically enhanced access control to shared resources. Personality-based encryption is, for example, a promising encryption approach for building smart data sharing systems. Anyway, access to management is not a versatile solution. In such cases, if your permission is revoked from the database, it must be completely revoked from the cloud server, and you will not be able to retrieve your information once it has been revoked. It has many features of realizability, usefulness, and effectiveness and thus shows the correlation that shows the proposed method diagram used to build a practical and intelligent data provider structure.

INTRODUCTION

Data sharing has become a ubiquitous aspect of modern life, however, with increased connectivity and data exchange comes with increased security risks. To mitigate these risks, various encryption techniques have been developed to protect sensitive information. One such technique is Revocable-Storage Identity-Based Encryption (RS-IBE). RS-IBE is a powerful encryption mechanism that enhances the security of shared data by combining the advantages of Identity-Based Encryption (IBE) with the ability to revoke access to encrypted data. Secure Data Sharing using Revocable-

DOI: 10.4018/978-1-6684-6646-9.ch005

Storage Identity-Based Encryption (RS-IBE) is a cutting-edge encryption technique that enhances the security of shared data. It combines the benefits of Identity-Based Encryption (IBE) with the ability to revoke access to encrypted data, ensuring that only authorized users have access to sensitive information. RS-IBE allows for secure data sharing across multiple platforms and devices while maintaining the privacy and confidentiality of the shared information. IBE is a type of public key encryption that uses a user's identity, such as an email address, as the public key. This eliminates the need for a public key infrastructure, making it a more efficient and scalable solution for data encryption. RS-IBE extends IBE by incorporating the capability to revoke access to encrypted data, ensuring that only authorized users have access to the sensitive information. RS-IBE is particularly useful for secure data sharing across multiple platforms and devices, as it enables the encrypted data to be stored in a central location, such as a cloud storage provider. In the event that a user's authorization is revoked, the encrypted data remains secure and can only be accessed by authorized users. In this computational data storage a computer process which offers huge task that hold massive storage capacity with low value. This provides the customers who can obtain the service they require despite the time or location, and it does so across various domain, bringing considerable ease to cloud users. Data services in various domain applications among which it has many services provided by cloud computing and can deliver an effective and convenient process which distributes information that is shared across the network and provides significant advantage for the users. Moreover, it is vulnerable to a number of security issues, which are among cloud customers' primary concerns. Users may be reluctant because outsourced data typically contains efficient and important informative data. Second, the data is shared commonly and carried out in an extended atmosphere, rendering data services susceptible to cyber-attack. Moreover, the cloud server itself may be used to illegally profit from the data of its users. Finally, shared data is not in fixed process. Which is when the user authentication has expelled, they will not be able to access previously and subsequent shared data. As a result, when information is delivered to a data hostile in which the user will be able to manage the data in which users who are currently permitted to share the information. Confidentiality and backward secrecy can be provided by a data sharing system. Moreover, the methodology of decrypt and rewrite the encrypted data which ensures safety and security . This comes with other hurdles . Indeed users or the people who authorize require the key decrypt-then encrypt the process that involves the use of users' private key information, making the entire shared data through which it forms threats. The data provider must frequently repeat to do decrypt-encrypt process while uploading file procedure to make sure the encrypted message of the shared data up to date. This method has a high communication and compute cost, rendering it difficult and not reasonable for customers in limited and computed and warehouse capacity.

A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare

Kenneth J. Boyte (2019). *National Security: Breakthroughs in Research and Practice (pp. 108-125).*

www.irma-international.org/chapter/a-comparative-analysis-of-the-cyberattacks-against-estonia-the-united-states-and-ukraine/220878