Chapter 27
A Secure and Privacy-Preserving Approach to Protect User Data across Cloud based Online Social Networks

Neelu khare
Vellore Institute of Technology, India

Kumaran U.
Vellore Institute of Technology, India

ABSTRACT

The tremendous growth of social networking systems enables the active participation of a wide variety of users. This has led to an increased probability of security and privacy concerns. In order to solve the issue, the article defines a secure and privacy-preserving approach to protect user data across Cloud-based online social networks. The proposed approach models social networks as a directed graph, such that a user can share sensitive information with other users only if there exists a directed edge from one user to another. The connectivity between data users data is efficiently shared using an attribute-based encryption (ABE) with different data access levels. The proposed ABE technique makes use of a trapdoor function to re-encrypt the data without the use of proxy re-encryption techniques. Experimental evaluation states that the proposed approach provides comparatively better results than the existing techniques.

INTRODUCTION

The advent of modern technologies facilitates the growth of social network sites in an increased manner. The term social network represents a social structure that maps the relationship between individuals. At present, there exist numerous social networking sites such as Facebook, Twitter, Instagram, LinkedIn and MySpace. In recent years, online social networks have become an effective platform to share messages as it becomes an inevitable part of our day to day life. This widespread adoption of online social

DOI: 10.4018/978-1-7998-7705-9.ch027

networks generates a huge amount of data every day in an increasing manner (Cheung et al., 2011; Gross & Acquisti, 2005; Kumar et al., 2010). The data is often generated from distinct sources in multiple formats. This creates the requirement of high computation power and large storage capabilities enabling the online social network systems to adopt cloud computing systems. Further, the storage and analysis of the data generated from the social networks provide numerous benefits to the society in several aspects such as business, education, banking, etc. This encourages the new ways to store and analyse real-time cloud based online social network data (COSN) in an effective manner (Garton et al., 1997; Benevenuto et al., 2009).

Even though the cloud based online social network systems be effectively used to better understand the world and innovate in various strands of human endeavors, the explosive growth of data increases the threat of data privacy (Mislove et al., 2010; Kim & Hastak, 2018). For example, the social networking sites such as Facebook and Twitter can store data user's sensitive information's such as personal life and social relationships for commercial purposes. This leads to privacy and security threats across the online social networking systems. Some of the circumstances in online social networks that lead to privacy breaches are described as follows:

- Some of the user's personal information's when combined with external datasets may lead to the inference of sensitive information about the user. This detail can be highly confidential and the disclosure of it may lead to serious privacy concerns. For example, leakage user health information.
- The user's personal information's are sometimes gathered and utilized to improve the business needs. For example, analysing shopping habits can add extra value to the business.
- The process of collection and storage of user sensitive data in an unsecured distributed or centralized environment lead to data leakage in the data storage and processing phase.

Since the data generated from the social networks are extremely large and complex in nature it is often referred to as big data. In order to protect data privacy measures across social networking systems, several approaches have been developed in recent years. However, the adoption of privacy-preserving techniques often varies at each stage of the big data life cycle (Freedman & Jin, 2017). In general, the big data mining process includes three phases such as data generation, storage, and processing. Data falsification and access restrictions are the two major techniques that preserve data security in the data generation phase. Data falsification is used to falsify the original data before it is sent to the untrusted third-party member. Access restrictions limit the level of usage of private data. The privacy protection techniques during data storage phase include the use of standard encryption and cryptographic techniques. Attribute based encryption, homomorphic encryption and identity-based encryption are some of the widely used privacy protection techniques in data storage phase. Similarly, in data processing, the two major techniques anonymization and suppression are used to protect data privacy. The proposed approach mainly deals with the data storage phase and provides an effective solution to preserve data security and privacy across cloud based online social networks. This due to the reason that the privacy breaches in data storage phase are comparatively higher than the other two stages.

Access control techniques act as an effective tool to protect data privacy in cloud based distributed processing systems such as online social networks systems. In such type of systems, the passive privacy concerns are considerably more dangerous than active privacy concerns. The active privacy concerns deal with the privacy breaches that occur when the data user willingly transfers a data to the third party. Active privacy breaches occur when a data owner publicly shares their sensitive information's on online