International Journal of Information Security and Privacy
Volume 16 • Issue 1

Provably Secure Authentication Approach for Data Security in Cloud Using Hashing, Encryption, and Chebyshev-Based Authentication

Danish Ahamad, Shaqra University, Saudi Arabia*
Md Mobin Akhtar, Riyadh Elm University, Saudi Arabia
Shabi Alam Hameed, Shaqra University, Saudi Arabia
Mahmoud Mohammad Mahmoud Al Qerom, College of Computing, Science, and Engineering, University of Salford, UK

ABSTRACT

Secure and efficient authentication mechanism becomes a major concern in cloud computing due to the data sharing among cloud server and user through internet. This paper proposed an efficient hashing, encryption, and Chebyshev (HEC)-based authentication in order to provide security among data communication. With the formal and the informal security analysis, it has been demonstrated that the proposed HEC-based authentication approach provides data security more efficiently in cloud. The proposed approach amplifies the security issues and ensures the privacy and data security to the cloud user. Moreover, the proposed HEC-based authentication approach makes the system more robust and secured and has been verified with multiple scenarios. However, the proposed authentication approach requires less computational time and memory than the existing authentication techniques. The performance revealed by the proposed HEC-based authentication approach is measured in terms of computation time and memory as 26ms and 1,878 bytes for 100Kb data size, respectively.

KEYWORDS

Access Control, Authentication, Cloud Computing, Data Privacy, Data Security

1. INTRODUCTION

In the increasing era of network and computer technology, the cloud computing framework emerges as the on-demand service through internet. Various cloud services are recently available based on the applications and data outsourcing. Hence, the users are aimed to store the information in cloud in order to minimize the cost and user burden (Jiang, *et al.,* 2018). The cloud computing model is quickly increasing in the field of industry and realizing the power of shared resources in the network environment, as it helps to drive the efficiency and savings of data. Despite of various advantages, data security and privacy are still concerns as open discussion in cloud. Thus, to provide a robust security solution in cloud becomes an important and significant area for research. In the network environment of economic conditions, the industries using the cloud services are grappling across the globe with the pressure of cost. However cloud computing services helps to minimize the expenditure of Information technology (IT). The world is tending towards the emerging trends, like cloud computing, the concerns regarding the privacy and security of information and other security issues should not

DOI: 10.4018/IJISP.2022010106

act as the barrier for adopting the cloud services. However, the cloud storage system allows the users to store and share the data with different access roles and permissions. In the precedence based data sharing model, each user has the access policy mechanism in order to access the file, and each file has the access rights to access the file such that the access policy may differ for various users (Agarwal, *et al.,* 2020; Kumar, *et al.,* 2020; Altowaijri, 2020; Shajina & Varalakshmi, 2017).

The cloud computing approaches greatly modifies the way to share the information in daily life. It is considered as the ubiquitous concept sharing model, as the subjects can use the devices in order to request the resource from different cloud servers. Thus, the security is concerned as an important factor in cloud (Fang, *et al.,* 2020; Farjana, *et al.,* 2020; Yang, *et al.,* 2017). To enable the authorized users to access the services in cloud, different cryptographic protocols, namely user authentication approaches are commonly introduced in cloud computing environment. These methods are integrated with the key exchange approach (Diffie & Hellman, 1976). in order to generate the shared session key that guarantees the security in the data communication scenario. In the existing scenario, the authentication approach based on the password model is the widely used measure in cloud (Wazid, *et al.,* 2020; Roman & Gondim, 2020; Ibtihal & Hassan, 2020; Lin, *et al.,* 2003). Here, each user can select the password and register then to cloud server. After completing the registration process, only the legitimate users can access the resources from cloud server. Moreover, the cloud server maintains the table called password table, that records all the information about the authenticated users and it increases the risk in leaking the password. To amend the security weakness, the server applies the hashing function for user password before it gets stored in the table. The malicious adversary user can obtain the hashed password and plot the password guessing attack by deriving the real password of users. To solve this issues, various user authentication approaches is introduced without maintaining the verification table (Lin, 2018).

The access control and the authentication mechanism are widely used to secure the outsourced data. Some of the existing research work focuses in key distribution based on the cost (Boneh, *et al.,* 2004). The advantages of security mechanisms are implemented in the single owner scenario. However, in the single owner scenario (Wong, *et al.,* 2000), the owner of the group authority of data has the right to modify, edit, and store the data in cloud. In the multi owner model, it offers more flexible for various applications at real time. However, all the owners present in the group has the rights to change, edit and read the fraction of information from the entire file that is shared by the organization group (Wang, *et al.,* 2013). These groups are dynamic in personality, as new user can join to the group by replacing the existing one, and the access rights can be revoked by the new user from the existing one. By changing the membership in the organization groups makes the data sharing more secure by eliminating the external users. Various cryptographic mechanisms, like data public auditing protocol (Yang & Jia, 2012), access control mechanism (Ruj, *et al.,* 2013), data possession protocol (Wang, 2012), key management (Barsoum & Hasan, 2012), and secure data sharing protocol (Liu, *et al.,* 2012) are introduced to solve the security issues. Most of the research works are focuses on authentication mechanism (Sharma & Banati, 2020; Abuarqoub, 2020; Shajina & Varalakshmi, 2017).

This research is focused to model a new HEC-based authentication approach to offer data security among the cloud user and server. The proposed approach consists of three different entities, such as cloud server, user, and the Authorization center (AC). The authentication framework is enabled using three different phases, such as registration phase, authentication phase, and data delivery phase. In the registration phase, the server creates its own credentials and verify with the AC using the session password. Similarly, the cloud user creates the credentials and verifies them with the cloud server. After registering the credentials of user and server, the authentication framework is carried out in the authentication phase. Here, the authentication messages generated by the user are verified with the server, while the authentication messages generated by the server are verified with the AC. Finally, the data is exchanged from the server to the user at the data delivery phase. The server encrypts the data using the user secret key and the data encrypt key and deliver the secure data to the user. Finally,