ABSTRACT

One of the fastest-growing and emerging applications among various computing industries is Big Data analytics. The volume of Big Data is increasing day by day in certain applications like healthcare, surveillance and agriculture monitoring. To persist, maintain and manage the Big Data, the cloud data centers are highly recommended. It is well known that the cloud doesn't provide complete security in terms of data and data access. Due to volume, velocity and variety of big data, data security and privacy issues are increased. Big data are an essential need for enterprise companies looking to connect their commercial potential. Since the growth of Big Data is endless, malicious activity over the data is also increased. Data generation is very fast and it is generated from various sources. Malicious activity has been focused on collecting the search history of web browsers, credit/debit card payments, pinging from mobiles through nearest cellphone towers etc. Using sensitive information any accidental/un-authorized disclosure of the data makes more serious consequences for the enterprises in terms of financial or business formula, which makes a huge loss of customer trust. So, industries are not willing to use cloud data centers to share secret and privacy data.

In order to provide a better solution for the above-said problems, various private and public cloud services provide key generation and sharing methods for data security. Some of the companies store their data in an unreadable format, where it cannot be used by the malicious users and it will not leak out the company data. But still, the security level is low and due to that enterprises meet data loss and leak.

Authentication, authorization, confidentiality, availability, integrity and privacy preservation are the greater focuses applied against security threats. Data sharing among several various parties for various tasks is critical in so many real-time applications like medicine research, homeland security and environmental protection. Several earlier research works have been proposed for providing security, but still there is a need for improving the security level. This research work focuses on providing a complete security in terms of optimized access control using Extended Artificial Immune System approach and Hybrid Access Control approach. Extended Artificial Immune System approach concentrates on optimizing the attributes of the data to tighten the access control security and it is suitable for any kind of big-data under cloud computing. In the first level it proposed a method to read, preprocess the data, extract feature, select optimal feature for knowledge discovery on the Big Data. Also, it generates dynamic authentication key for user validation and authorization for data access. Each user is assigned with the user code generated based on the nativity of the user and it never conflicts with other user code. Since, unique level of user code is used for user access permission provision, it increases the security efficiency. Hybrid Access Control is designed by integrating role based access and location based access control method for increasing security in cloud environment. The above cognitive technology is used to evaluate the proficiency of correct and incorrect login of users, percentage of data leakage, key generation time, time complexity of access control and percentage of malicious activities and the results are simulated and depicted. From the above validated measures, Hybrid Access Control provides higher security than other approaches like Bucketization, Subset Cover Method ,Role based Access Control, Location Based Access Control and Extended Artificial Immune System techniques for data analytics in cloud environment.