ABSTRACT

Identification and Access Management (IAM) has developed into a critical facet for achieving business enterprise benefits from the perspective of the management of digital or electronic identities, access control and business growth of organizations. Many business organizations widely adopt Cloud computing for its capacity of enabling universal and convenient, network access on request to a shared pool of configurable computing resources, IAM is considered as the prime layer of security in the cloud. Managing user's identity and providing adequate privacy and security in the cloud is a great challenge. These challenges gained increase in the research attention.

The objectives of the research is to investigate security issues in cloud, to identify various IAM approaches, access control mechanisms to build IAM services, design models using various access control schemes to achieve IAM services in the cloud and assess the IAM schemes.

The investigations were performed on the applicability of cloud for health care which describes the concept, challenges, and solutions of IAM and on various schemes for implementing IAM. The key limitations identified in the current approaches of access control are (i) Discretionary access control does not have any control on the access flow of information and these information are copied into one to one objects; therefore it is possible for an external user to access the original copy of information even if the owner does not provide the access to it. (ii) Mandatory access control model has restrictions on user access and dynamic change in security policy is not allowed. (iii) Role based access control defines the roles of the object in a different context in distinct forms, it is difficult to adopt in dynamic

environments. This necessitates the development of attribute based access control for IAM with emphasis on the research issues namely data confidentiality and data integrity.

The work endeavours to design and develop authentication, access control and user management for IAM as a service in the cloud. The basis is investigations performed on existing methods and considerations with regard to security issues. Strong authentication, access control and user management are well ascertained by attribute based encryption; users are granted access rights through access policies which combine attributes together and to update the access policy by modifying the old access policy to new access policy during the model development.

Enhanced access control schemes based on attributes are designed and developed to realize IAM in healthcare cloud. Attribute-Based Encryption is a cryptographic technique that uses access policies and attributes with cipher texts and private keys to support access control over encrypted text. “Modified hierarchical cipher text policy attributes based encryption and attribute based signature” scheme is designed to permit the access policy to be defined by the owner of the data over a universe of attributes in the cipher text wherein the data is decrypted by the user. The results of the proposed scheme show that the encryption time is constant even if the number of attributes is higher than the earlier schemes, in which it shows that there is a linear growth in the number of attributes in the accessibility tree along with an increase in encryption time.

To dynamically change the access policies after decryption of data, “Modified hierarchical cipher text policy attribute-based sign encryption” scheme is designed. The performance of the MHCPABSC scheme is

compared with the MHCPABE and ABS. The proposed MHCPABSC shows the cost of MHCPABSC is less than the cost of MHCPABE and ABS in unsigncryption. The correctness of the security property ensures this model is collision resistant.