ABSTRACT

Cloud Computing is renowned for hosting and delivering Information Technology enabled capabilities as services on-demand based on internet technology. This computing paradigm gains more attention due to its significant characteristics like on-demand self-service, resource pooling, rapid elasticity, broad network access, and flexibility, at reduced cost that helps individuals and enterprises to fulfill the changing dynamic infrastructure demand without the burden of building, managing, and maintaining it internally. Nowadays, organizations and individuals desire to outsource data and computations in order to alleviate the complexity in handling business processes internally with the available infrastructure on hand. As cloud offerings are prominent and felicitous for today’s business, organizations and individuals plan to leverage cloud computing for outsourcing, which facilitates data owners to acquire storage and compute resources on-demand at reduced operational cost. Even though cloud offerings are tremendous, one key aspect that hinders the adoption of cloud by many data owners is concern over security and privacy.

Since the hosted data resides on shared servers at third party’s premises, data owners lose control over their data and computations and have to depend completely on the cloud service provider where the service and management of data may not be fully trustworthy. Data owners are not aware of the migrated data that is being exposed to various internal and external attacks due to the multi-tenancy nature of cloud. External attacks are initiated by malicious users outside the cloud environment who is capable of compromising cloud servers. Insiders’ attacks are carried over by the privileged users at the cloud service provider’s site and such attacks are very
difficult to detect. Sensitive data stored in cloud servers either intentionally or accidently leaked by these privileged users causes serious loss to data owners. Therefore, cloud is basically insecure from data owner’s viewpoint. On the whole, concern over confidentiality, integrity, availability, privacy, and authenticity are the key aspects that prevent data owners to move their data into cloud storages.

Though cloud model has enormous benefits, unless concern over confidentiality and integrity are addressed, many of the potential customers will be reluctant to adopt cloud model. This thesis seeks to address cloud data security problems and renders appropriate data security solutions for concerns over confidentiality, authenticity, and integrity of data. To mitigate data security concerns, in this thesis, secure and efficient protocols based on Elliptic Curve Cryptography for multilevel security in cloud environment to preserve confidentiality, authorized access to stored data, authenticity and integrity of data from the perspective of data owner is designed and developed. The core work of this research work is elucidated below.

**An Adaptive Multi Level Security (AMLS) Framework to Secure Cloud Data:** To protect the data outsourced to cloud data storage, it is proposed to enforce Multilevel Security which improves data confidentiality contrary to single security system and any common multiple security system for the whole data. The necessity for data classification and encryption combined with other primary security measures are outlined exhaustively. The responsibilities of data owner and methods to protect their data stored in cloud are also elucidated in this research work. The AMLS framework has been structuralized to combine various techniques and to utilize them to perform appropriate security task that is adequate to protect data stored in untrusted cloud storage from the perspective of data owners. Especially to exhibit the importance of data classification and encryption, in this research work, the classified data with different file sizes are encrypted with various
encryption algorithm and is tested in a private cloud environment deployed using the open source software “OpenStack” and the performance of these algorithms are analyzed to find the encryption algorithm that is felicitous for massive data to be outsourced to cloud storage.

**Elliptic Curve Cryptography based Adaptive and Secure Access Protocol (ECC-ASAP) for Cloud Data:** The ECC-ASAP is designed to let the data owner and the data users in a hierarchy to authenticate mutually and let data users to derive secret key and access the data stored in cloud data storage. ECC-ASAP ensures that the data outsourced to cloud storage is made available only to the authorized users thereby holds fine-grained access to resources.

**Efficient and Secure Elliptic Curve Cryptography based Digital Multi-Signature (ECC-DMS) Protocol:** The ECC-DMS protocol ensures authenticity of data that is shared between different groups of users. Users belonging to a group or security class needs to share and process the stored data. Such data requires to be authenticated by all users in that group, which is verified by data owner so that users belonging to other groups or security classes can use it. The ECC-DMS protocol efficiently ensures the authenticity of data shared between different user groups.

**Elliptic Curve Cryptography based Provable Data Possession (ECC-PDP) Protocol with data dynamics for secure cloud storage:** This research work outlines the problems related with provable data possession schemes in cloud environment and provides provable solutions to verify the integrity of data in cloud data storage. The ECC-PDP protocol aims in preserving confidentiality of outsourced data and allows dataowner to verify the correctness of data without retrieving the whole original data from cloud storage which reduces the communication overhead. Also, the protocol provisions stateless auditing by challenging the cloud server to prove the data possession and also supports data dynamics at blocklevel while retaining the
same security assurance. The stateless auditing relieves verifier from maintaining the states between audits which is a desirable property. The security and performance analysis proves the proposed protocol to be secure and efficient for secure cloud data storage.

The protocols in this research work are designed using Elliptic Curve Cryptography (ECC) to obtain two main advantages, that is, improved security and performance. ECC provides higher security with shorter keys compared to other asymmetric algorithms. The solutions provided in this research work for cloud data security, alleviate the data owner’s fear over malicious attacks on data outsourced to cloud data storage. The security analysis and performance analysis proves that the ECC-based protocols are secure and efficient and helps data owners to defend their data against malicious internal and external attacks in cloud environment.