1.1 Introduction

Advances in the field of Information Technology has influenced outsourcing of information and sharing. Social networking websites and e-documents offer an easy method for users to outsource and share diverse information on the cloud storage servers such as photos, events, news, etc. Cloud Computing arises to be the future of IT architecture, thus it provides unlimited and flexible resource for storage in cost efficient manner [1-4]. The early period of Cloud Computing itself gained immense attention and has also attracted enormous users to transform their data centers present locally into cloud servers present remotely.

One of the most critical issues in storing data remotely is data security. On one side, it is necessary to strictly protect sensitive information before allowing the users to use the appropriate data services. On the other side, users do not have their data physically in remote data storage.

In traditional methods of access control, reference monitors [5-8] can be completely trusted but remote data servers cannot be trusted by users to implement access control policies. Thus a user enforcing data access control is required for remotely storing the data. Various cryptographic methods allow the user to implement data access policy where the encrypted form of data is stored on the servers which retains the secret key(s), the user control access is established by giving the equivalent data decryption keys. In untrusted storage, Attribute-Based Encryption (ABE) provides the best cryptographic foundation for a securing data sharing schemes.

1.1.1 Cloud Computing – An Overview

Cloud computing technology delivers the computing resources through internet. In cloud computing technology, the computing resources are all shared and the clouds are divided into several types based on the locations of the users [9]. The public clouds are either free for usage or paid based on usage. They owned and functioned by the cloud providers. Social networking services, e-mail services, online storage services, etc are all few best examples for public clouds. The cloud
infrastructure of private clouds deals entirely for a particular company, and is handled by that company or a third party. Eucalyptus, VMware, Elastra, Microsoft, etc are all few good examples for private clouds. The community clouds, shares the services of two or more companies and is obtainable to that group only. The infrastructures of the community clouds are handled by service providers or the group of companies. Hybrid clouds are the clouds that combine several methods of resources.

There are three service models based on cloud computing which are SaaS, PaaS and IaaS. The SaaS denotes the Software as a Service, PaaS denotes the Platform as a Service and IaaS denotes the Infrastructure as a Service.

1.1.2 Types of Cloud Computing

- **Software as a service (SaaS):** SaaS is delivery application on the Internet. Without the software installing and maintenance, the services access is direct through the Internet, without intervention of software complexities and management of hardware.

- **Platform as a Service (PaaS):** PaaS represent a layered part of the software. In PaaS, the developing environment is combined and the services are given, which are used in building higher service levels. The applications can be built by the customer itself and works on the infrastructure of the provider. It offers an already defined of operating systems and application servers, like LAMP platform which denotes Linux, Apache, MySQL and PHP, Ruby, J2EE, etc.

- **Infrastructure as a Service (IaaS):** The fundamental storage and computing functionalities are provided by the IaaS. The customers organize the software’s to the infrastructure. Amazon, 3 Tera, Go Grid, etc are dew best examples of IaaS.

1.1.3 Basic Cloud Characteristics:

- The information on infrastructure, application interfaces through the APIs need not be known.

- The elasticity and flexibility makes it possible for scaling up and scaling down which utilizes all the resources like storage, capacity of server, load balancing, database management, etc.

- The cloud services can be used and paid as per the usage and needs.

- The cloud technology can be used anywhere at any time based on network.
• The clouds are clear to the users and also transparent to the applications, thus are used to build branded multi way products, open source environments, software’s, hardware’s, etc.

1.1.4 Cloud Security Issues

There are numerous security problems and challenges in cloud computing technology. The security problems on cloud computing is specified in [10]. It is necessary for the network on the cloud which is responsible for interconnection among the systems to be safe and secure. Cloud computing has virtualization patterns which gives rise to many security problems. Thus to map virtual machines into physical machines, a high security is required. The data securities include encryption of the data and ensures relevant policies needed to carry out data sharing. The allocation of resources and the memory managing algorithms should be highly protected and safe. One of the major problems in cloud computing is that it implicitly consists of the business critical data and complex processes and also outsources sensitive data securely. The data stored on a cloud service is the responsibility of the cloud provider who controls and protects those data. When the data is organized on the cloud through IaaS or PaaS, then the complete control is possessed by the cloud provider. For this reason, a trust worthy relationship among the cloud users and the cloud service providers is required for which several researches are carried out.

The security threats faced by most of the computing systems are all also faced by the cloud computing technology. The main problem in outsourcing the data present in the mobiles is misusing of the data or violating the integrity of the data. Protecting the confidentiality and sensitive files that is outsourced is one of the major issues [11, 12]. The processed files present in cloud storage are kept away from the illegal users by utilizing the attribute based encryption for controlling the admission of the files being encrypted by the Data Owners. Attribute Based Encryption is a method based on cryptography which provides better security, secrecy of data, and prevents several attacks. The first ideology of Attribute Based Encryption was developed by Sahai and Waters during 2005 [13]. Later many improvements on Attribute Based Encryption techniques were evolved. The methods of access policies are divided into two types, key policy ABE model and cipher text policy ABE model. The ABE scheme consists of data owners, certificate issuers, and receivers. The work of the issuers is producing
the keys for the Data Owners and the work of receivers is the ciphering and deciphering of data.

The verification of Remote Data Auditing verification is another significant security aspect. Many researchers came up with several models and security techniques. PDP which denotes Provable Data Possession was developed by Ateniese et al. [14] in 2007. According to the Provable Data Possession model, the auditors are capable of verifying the authenticity of the files. Two safe Provable Data Possession techniques were developed using the rijndael model. A vibrant Provable Data Possession model without insert operations was developed by Ateniese et al [15]. Then many RDA models were developed [1-3, 16, 17, 18]. The first Proof of Retrievability models with better security was developed by Shacham in 2008 [4]. According to Proof of Retrievability’s models, it is possible for the author to obtain the data and also check the realness of the data. The original works on these models is specified in [19, 20, 21, 22]. Sometimes the users hand over’s all the verification work to Third Party Auditor in Cloud Storage Technology, this technique is also known as Third Party Auditing [23, 24, 25, 26].

1.2 Research Background
1.2.1 Protective Data Distribution in Cloud Platform

Cloud computing technology offers elastic resources and limitless resources like storage space and various services. In Cloud Computing technology both the users of cloud services and the providers of cloud services are mostly different from each other trust domains. Secure access control should be given before the cloud users and has the freedom for subcontracting susceptible data necessary for storing. Therefore the data owners take complete control in the data access. In Cloud Computing technology, cloud users can also be resource controlled devices like mobile phones. Thus, to minimize the totaling load for cloud users, certain delegation techniques and protectively offload computationally serious tasks to cloud servers. The computation load is reduced using the techniques of lazy re-encryption [13] for the data consumers to the complexity and also made it affordable for the user devices like mobile phones. Also, both the security proofs and analysis of performance are provided.
1.2.2 Policies for Data Accessibility in Shared Cloud Storage

By storing the data on the local servers or at the designated networks such as cloud servers, several benefits like cost, efficiency, easy retrieval of distributed data and saving the network communication load can be achieved. The cloud servers which are not accessed are easily exposed to severe attacks like physical compromises. They are also not trusted by the cloud owners for data security. For this reason in cloud servers, protected data storage and retrieval mechanism is needed for distributed data storage. Thus, this thesis provides cryptography based access control methods like encryption of data on the cloud storages using public keys and distribution of decryption keys to approved clients. The operations are distributed to all these phases for making ABE encryption operation techniques inexpensive to the cloud entities. The existing ABE scheme is revised and the user revocation complexity is made constant for minimizing the computation and communication load present on the system entities.

1.3 Problem Statement

Data storage servers are not permitted to use the sensitive data and cannot enforce data access policies in untrusted storage. For this purpose of maintaining the confidentiality of the data, the owner of the data does encryption of the data before uploading them on the servers. A data decryption key(s) is provided to grant the user control access. There are also some challenges faced by the cryptographic access control methods, which are as follows

1.3.1 Fine-grained Accessibility Control against Scalability

Multiple users can have access rights to various types or different chunks of data using fine grained access control. Data servers in general imposed access policy with several mechanisms like ACL-based access control [6], access control based on role [8] and access control based on capability [7].

Access control based ACL has certain scalability issues and requires all the data object to store the catalog of all users who are authorized. ACLs are less scalable by enforcing cryptographic methodology such that complexity of the data objects regarding its size of cipher text size and data encryption operation is linear with respect to users. Capability-based access control also has the same scalability
problems. In the access control based on role [8], entry is given depending on the user’s activities and authorized user’s list need not be maintained. When these access policies are imposed along with various cryptographic methods, it faces several attacks like user collusion where different users try to fetch extra privileges.

Based on these issues in data access control which uses cryptography based on symmetric-key or public-key, numerous researches are made recently [12,13,24,25]. For fine-grained data access dealing with large data and several users, these schemes are not much suitable. Fine-grained access policy for large systems can be implemented using ABE [18, 27, 28] where one-to-many public-key cryptography is possible. Inside the encryption procedure various access policies based on attributes are implemented. Encryption of data without receiver set knowledge is possible in ABE. In For this reason, ABE is associated with Role-Based or Attribute-Based Access Control methods which are used for large applications. Presently ABE [18, 27, 28] works on the basic functions like, data encryption, data decryption and also collusion resistance.

1.3.2 User In-Out Flexible System

For granting user access privileges and for providing revocation, an efficient and effective user management methodology is required. Cryptography and ABE always faces a challenging issue in user key revocation. Certain presented solutions [17, 27] provide a suggestion in linking the user secret keys to expiration time attributes. At the designated time, these solutions are capable of withdrawing user secret keys, but are not capable to withdrawing users in a timely manner. Prevention of existing files from a revoked user’s access is not done in a data or file storage. For this purpose, it is better to use real time communication.

1.3.3 User Authenticity

In cryptographic-data access control, user access is provided by assigning the data decryption keys. Thus it is possible for a malicious but authorized user to share the secret key with an unauthorized user. In applications that are copyright-sensitive it is even possible to sell the secret keys with all privileges to other users. These attacks are very dangerous because duplicating and distributing the decryption keys by email is very easy and less costly for key abusers rather than distributing data directly.

6
Even though preventing these attacks completely is difficult, it is possible to give data owner a technique in tracing few doubtful pirate devices and gather some evidence of abuse by revealing the illegitimate key distributor’s identities before the law. Thus a user’s decryption key is somehow associated with their own identity. The traitor tracing is a technique used to address the issuing of key abuse [29-32]. In an Attribute based encryption [18, 27, 28], the secret key is assigned along with its attributes and it will not have a one-to-one relation with any user. At a higher level traitor tracing is done to protect against abuse attacks in ABE. ABE is not applicable to the existing techniques of traitor tracing systems because their receivers are being represented independently in conservative broadcast encryption. For this reason, a good solution is required for protecting against key abuse attacks in ABE. Thus the major challenge is to correctly perform tracing activities such that suspected users do not detect.

1.3.4 Protection of Data Confidentiality

It is necessary to reveal less user’s private information in addition to the data confidentiality because data storage servers cannot be completely trusted. Attributes or access policies are needed to be joined in the plaintext to the data cipher text in order to assist the user decryption in the present implementation ABE [18, 27, 28]. Access policies and attributes can be hidden to preserve privacy by providing a newer implementation of ABE. Efficiency is an application challenge because it is different for all applications as per their requirements. The recent ABE implementation introduces a mechanism which pairs the encryption and decryption. They are very expensive and thus unaffordable. In order to delegate computationally intensive operations in powerful systems, it is necessary to merge ABE along with several delegation techniques.

1.4 Research Objectives

The prime objective of the work is to design and develop architecture for mobile computing where Attribute Based Encryption technique can be used seamlessly and can provide fine grained access control to the users even at the time of user revocation and rekeying.
Key objectives of research include:

- Analyse major symmetric cryptographic techniques on mobile environment to find best efficiency algorithm.
- Research on different mechanism involving mobile data outsourcing on servers which provide access control methods.
- Design and develop architecture which could be able to keep privacy of mobile user data on server using advanced ABE mechanism and also provide fine-grained access control.
- Use Java language for web programming and android for mobile device apps as both the most popular in their segments.
- Compose a complete thesis on study and incorporate experimental results.

1.5 Research Motivation

In this research situations were considered where user need to outsource their data using their mobile device to online web servers like cloud storage and the data sharing should happen within certain user groups. As the privacy of data is a matter of concern on untrusted servers, users need to make sure their data is in safe hands. There should be a mechanism through which the control on servers can be limited and multiple entities can be involved in making the system more secure and resilient. There are few works done prior to implement ABE (which is most advanced mechanism in this field) in web applications, but still there is very limited work done to integrate this mechanism where users access the services using their mobile devices.

1.6 Research Contributions

ABE is a new technique for mobile computing which provides cryptographic methods based on data access control. Before the application of ABE to practically used systems, many issues should be addressed. This thesis addresses such issues and gives rise to multiple security enhancements.

- Revocation of User Access Rights

This is one of the most challenging issues for ABE because attributes are shared along with unlimited mobile users. One user’s revocation involves
key updates for other users who are not revoked servers. In order to make possible this user revocation on untrusted storage, a data owner is capable to withdraw any of the users in a timely manner. Data owners are able to protectively offload computationally intensive activities to powerful user revocation to the data servers. This is achieved by joining proxy re-encryption mechanisms [33] with ABE. The security of this proposed system is proved under the standard cryptographic models.

- **Efficient Keyword Search**

  As the mobile user files are encrypted before putting on server storage disks, there are lots of efficiency issues in deriving the ranking of relevant files as per the frequency count of keyword. Multi keyword search can be a tedious task on any of the search mechanisms. In addition to that if synonym matching is again conducted on every keyword then the complexity increases by many folds. This problem is common with data outsourcing on remote servers and particularly mobile devices suffer especially due to its resource constraints. We propose a novel mechanism to identify and retrieve most relevant information with efficiency. Test results prove the accuracy and efficiency of proposed technique.

- **Encryption with Access Policy**

  In current CP-ABE implementations [27, 34], the access policy should be attached in plaintext to the data cipher text in order to facilitate user decryption. This plaintext discloses the data owner’s access policy and or the users’ access privilege, and may cause privacy concerns. In order to provide better privacy protection, we propose diverse CP-ABE implementations under different security models. These solutions hide the access policy information not only from the data servers, but also from users.

1.7 **Scope of the Thesis**

The periphery of this research is within the following scope:

- To do a complete research on various ABE mechanisms and data security techniques.
• To derive a solution for mobile users that improves data security mechanism on server.
• To design and develop a model architecture through which proposed solution can be assessed.

1.8 Outline of Thesis

Chapter 1: Introduction: This chapter introduces about the concept of overall research. It gives general idea about the present scenario and issues concerned within it. It defines the objectives of this research, motivation behind it, proposed mechanism as contribution, scope of this thesis and outline of all the following chapters.

Chapter 2: Review of Literature: This chapter provides basics of mobile cloud computing, uses of thin devices in cloud computing, various security mechanisms and techniques being used currently, advantages of mobile cloud and the issues involved. This chapter also discusses about basic cryptographic techniques basics in any data security and AES algorithm was chosen for all the encryption purpose throughout the research, after thorough research on various cryptographic mechanisms and found it best for the work. It was the first module of the research work to find best suitable cryptographic algorithm. At the end of this chapter an understanding of Attribute Based Encryption (ABE) is summarized.

Chapter 3: Materials and Methods: This chapter explains about

A) Implementations done for privacy preserving ABE under standard group model and XDH supposition. It gives introduction to the system model used and assessment of it for security and performance with outcomes.

B) Secured sharing with ABE on Cloud, its information on related works done by various researchers, explanation about the system and security models, design goals, idea behind proposed method, implementation of model and explanation, analysis of proposed system with security and performance analysis.

C) Security by Adapting Data Splitting in Multi-Cloud, security prospects by multi cloud approach, data storage on multiple servers, problems involved in it, the mechanism, architectures and algorithm implementation.
D) File Search in Mobile Cloud Computing, related works done in the past on multi keyword search on encrypted cloud data, our implementation of new system, algorithm involved in it and discussion.

E) User Revocation in ABE- problem formulation, various schemes proposed, proposed implementation of new scheme, stages involved in it and discussion.

**Chapter 4: Results and Discussions:** This chapter demonstrates results got from the work done in all the modules. All the module research assessments are demonstrated individually for clear understanding with scenarios and setups held. Comparisons are done to show the efficiency of proposed methodology and discussions are carried out on same.

**Chapter 5: Conclusion and Recommendations:** This chapter presents summarized conclusion of whole thesis. Future works section describes the limitation of this research and suggest the expansions that can be carried out on this research in future.