Chapter 4

RESULTS AND DISCUSSIONS

This chapter provides complete demonstration of results obtained through various experiments and model developments during research.

Entire experiments were carried out in four modules where first module was to ascertain which symmetric cryptographic algorithm among AES, DES and 3DES best suits for mobile cloud computing. Second module of the research is to outsource mobile data to multi-cloud environment with ABE. Third module of research is to find a way to search files which are in encrypted format on cloud using mobile device with multi-keyword query search. Last module of the study focuses on creating an architecture where files from multiple group users using mobile devices can be outsourced to cloud server using novel CP-ABE technique.

There is a concise and to the point explanation of each experiment conducted while doing research and obtained results. Assessment of outcomes is done to demonstrate the overall effectiveness of implemented model.
4.1 Architecture Design

![Layered Architecture ABE Diagram]

Figure 20: Layered Architecture ABE

Above layered architecture diagram demonstrates the overall proposed CP-ABE system for mobile computing. Top layer indicates thin devices used by various users of the system. These handheld devices use presentation layer UI components i.e. Graphical User Interface (GUI) and application layout using ‘activities’ in android. Presentation layer components make communication with business layer through service interface i.e. HTTP protocol and JSON objects to bind and transport data from server to client. Business layer has all logic components for calculations and processing operation which keep entities such as certificate authority, attribute authority and security components that uses AES cryptography. Server side layer has an interaction with dataset via data access objects, connection APIs and service agents for processing. Data sources are maintained to have connections with database. Security, operational management and communications are integral part of system which is utilized in all the layers.
4.2 Module 1

4.2.1 Abstract

There are immense numbers of clients who utilize cloud services through mobile devices, for example, mobiles, PDA, tablets, portable workstations because of its adaptability and portability characteristics. Mobile Cloud Computing has numerous favorable circumstances intrinsic in it however there are few dangers and imperatives that exists, for e.g. security, information access control, proficiency, data transfer capacity, and so on. Numerous cryptographic calculations are contemplated before offering secured and productive operations on web and standalone applications however symmetric algorithm usage on versatile environment is still under research. To contemplate the proficiency of different cryptographic security algorithms, for example, AES, DES and 3DES, these algorithms were executed on portable environment and through the outcomes obtained from continuous usage of these algorithms on different handheld gadgets, it is demonstrated that which cryptographic technique can give productive and dependable security system for information access control and security of client's outsourced information in mobile cloud computing.

4.2.2 Experimental Setup

Fundamental goal of this study was to outline a structural planning where information proprietor can outsource their information through cell phone with high proficiency and security. The primary calculations considered here were AES, DES and 3DES. Every one of the three calculations were executed on android dialect and were keep running on cell phones to check the effectiveness of these symmetric calculations. For execution measures three distinctive cell phones were utilized of different designs. Gadget arrangements are as per the following:

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Samsung Galaxy Tab 3 (Device 1)</th>
<th>Samsung Galaxy Star Trio (Device 2)</th>
<th>Samsung Galaxy S Duos 2 (Device 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Android 4.1.2(Jelly Bean)</td>
<td>Android 4.1.2(Jelly Bean)</td>
<td>Android 4.1.2(Jelly Bean)</td>
</tr>
<tr>
<td>Chipset</td>
<td>Marvell PXA869</td>
<td>Qualcomm MSM7225A</td>
<td>BCMBS45/28153</td>
</tr>
<tr>
<td>CPU</td>
<td>Dual-core 1.2 GHz Cortex-A9</td>
<td>1 GHz Cortex-A5</td>
<td>Dual-core 1.2 GHz Cortex-A8</td>
</tr>
<tr>
<td>GPU</td>
<td>PowerVR SGX540</td>
<td>Adreno 200</td>
<td>Broadcom VideoCore IV</td>
</tr>
<tr>
<td>Memory</td>
<td>1GB, 1 GB RAM</td>
<td>4GB, 512 MB RAM</td>
<td>4GB, 768 MB RAM</td>
</tr>
</tbody>
</table>

With the end goal of information stockpiling on server google's distributed storage administration was considered were each encoded information was being stored to the server.
4.2.3 Android App Screens

Encryption and Decryption

- AES_ALGO
- DES_ALGO
- 3DES_ALGO
4.2.4 Results

Extensive assessments were conducted to check productivity of symmetric calculations on portable environment for encryption and unscrambling of information before outsourcing information to cloud servers. Experiments include execution of algorithms i.e. AES, DES and 3DES when executed for various no. of operations all the while. The following are the outcomes of calculation execution which were found in study:

Device Performance on Algorithms

![AES Performance Chart]

Figure 21: AES Performance
Figure 22: AES Performance

Figure 23: DES Performance
Figure 24: DES Performance

Figure 25: 3DES Performance
Figure 26: DES Performance

Algorithm Performance on Devices

Figure 27: Device 1 Performance
Figure 28: Device 1 Performance

<table>
<thead>
<tr>
<th>Encryption - Decryption Rounds</th>
<th>3DES</th>
<th>DES</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>3551</td>
<td>477</td>
<td>1334</td>
</tr>
<tr>
<td>5000</td>
<td>15722</td>
<td>2146</td>
<td>6673</td>
</tr>
<tr>
<td>10000</td>
<td>29965</td>
<td>3868</td>
<td>12862</td>
</tr>
<tr>
<td>20000</td>
<td>61748</td>
<td>8087</td>
<td>28651</td>
</tr>
<tr>
<td>30000</td>
<td>95849</td>
<td>13380</td>
<td>43364</td>
</tr>
</tbody>
</table>

Device 1 Performance

Figure 29: Device 2 Performance

Device 2 Performance

AES
DES
3DES
Figure 30: Device 2 Performance

Figure 31: Device 3 Performance
4.2.5 Discussion

Having a profound study on execution of three noteworthy symmetric calculations i.e. AES, DES and 3DES on android based cell phones for information outsourcing on cloud, it is inferred that execution of DES is obviously better than other two calculations if there should be an occurrence of productivity and throughput. Execution of 3DES on security scale is not practically identical to AES and DES as 3DES takes as much as three times more handling time than DES however for the same time it gives three times more grounded security than DES calculation. For an ideal level of effectiveness and security even AES can be suggested as its proficiency is superior to 3DES and security wise it is practically identical to DES. DES is considered to be feeble among these three calculations in past researches. As cell phones lack in high resource contrasted with desktops and tablets, it can be summed up that AES may end up being a decent choice to execute on mobiles for better execution and security.
4.3 Module 2

4.3.1 Abstract

Cloud Servers offers the users with several services. One such important service is the services based on data storage. The users using mobile devices generally depend on such services in order to get better performance, mobility, and security. The mobile devices generally have less storage capacity for data when compared to the conventional computer systems. Thus the mobile service providers make it available for its user such that the data is stored remotely in order to access it when required and also for providing good security of the data. But one of the major concern of the mobile users is about the privacy of the data because the data is stored remotely on cloud servers. Thus the problems faced by the user in storing the multimedia data remotely, an Attribute Based Encryption architecture, and a multi cloud technique to reduce such problems are all identified. There are existing work already carried out on the privacy of data in a single storage severs but not many research is made on multi cloud servers. Experiments were conducted on the techniques of multi-cloud splitting of encrypted data and find the efficiency of system.

4.3.2 Experimental Setup

A mobile with android Operating system, an app allowing users for achieving various functions, one proxy server with tomcat are required for performing the experiments. To measure the efficiency of different file sizes, data with variable sizes ranging from 100kb to 500kb is selected.
4.3.3 Android App Screens
4.3.4 Results

![File Upload Time Graph](image)

**Figure 33: File Upload Time**
Figure 34: Binary Conversion Time

Figure 35: Encryption Time

Figure 36: Serialization Time
Figure 37: Fragmentation Time

Figure 38: SHA Hash Generation Time

Figure 39: Deserialization Time
There are many transactions in this experiment. The users can login and register to the homepage for uploading and downloading the files. The start time for uploading and the finish uploading time is calculated resulting in the total upload time. Then the time efficiencies of converting image into binary, encrypting, decrypting, serialization, retrieving, fragmentation, merge of fragments, generation of hash codes with SHA-1, and downloading are all calculated. Later the experiment is repeated for different size of files.

4.3.5 Discussion

A multi-cloud architecture model proves to be great advantage in storing contents on the cloud. This model enables better privacy, integration and security of the data. The efficiencies of SEF-MC algorithm for several data sizes are proved that it is capable to outsource via mobile devices by this algorithm. The sever scripts are deployed for configuring the hardware servers using internet, and thus provides better performance to the applications. Future works is done such that encryption can be done inside the mobile itself and still maintaining flow channel to be secure.

4.4 Module 3

4.4.1 Abstract

Cloud computing provide great improvements in storing and retrieving the data. The users of mobile phones have less storage due to the low capacity of memory, thus they use cloud storage technology. To maintain the confidentiality of the files present on servers, the files are encrypted using encryption techniques. After
encrypting the file on server, the decryption is not possible using the keywords of the previous files. Thus new techniques with enables both storing private files on the servers and also searching of the files are developed.

4.4.2 Experimental Setup

Experimental Results are done with this developed model using several data sets of different size of files. The valid plaintext files will be uploaded for later operations.

<table>
<thead>
<tr>
<th>File Size</th>
<th>50KB, 100KB, 500KB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keyword</strong></td>
<td><strong>Synonym</strong></td>
</tr>
<tr>
<td>Nature</td>
<td>Environment, ecosystem</td>
</tr>
<tr>
<td>Creature</td>
<td>Animals, living-beings</td>
</tr>
<tr>
<td>Mobile</td>
<td>Cellphone, phone</td>
</tr>
</tbody>
</table>

4.4.3 Android App Screens

![Cloud Search](image)
4.4.4 Results

Figure 41: Data Upload Time Graph

The graph represents the file uploading time and the analysis of keyword analysis. This chart shows the keyword searching time along with the frequencies of the synonyms. The experiment is done using many keyword searches which have two synonyms. The searching time is less when comparing it with the file uploading time.

Figure 42: Upload Time Chart
The figure shows a bar graph representation of the keyword’s TF searching time and uploading time along with Synonyms. The time little varies with the no. of keywords and its synonyms which are suppose to be found in the file to define the ranking.

AES algorithm is needed for encryption such that efficiency and security is combined and handled. The initial working needs only less time but thereafter encryption has took very negligible time.

Figure 43: Encryption Time

The figure below represents the result time of 1, 2 and 3 keywords. The 1 keyword takes 32ms for searching results, 2 keyword takes 73ms for searching and 3 keyword takes 166ms for searching. The processing is increased by 1 keyword which depicts 1+ 1*2 TF and 3+3*2 TF is depicted by 3 keyword
The figure below represents the decrypting time of the files and the connections from raw files to download is generated. After downloading the file, the file will be deleted by itself.

This model works on the mobile data that is encrypted on the cloud storage. The confidentiality of the data that the server stores and the efficiencies that use indexes are all assumed. The searching methods are not only restricted to keyword
queries search but also the synonyms of those keywords during ranking generation. Thus AES algorithm is used for better efficiency and security in cipher operations.

Further researches are made on searching methods based on Natural Language Processing. This model can be upgraded such that the keywords can be generated along with file ranking and related synonym.

4.5 Module 4
4.5.1 Abstract

With the advent of business applications which permits clients to frame dynamic groups, so that they can store information on cloud servers and offer the information within their client groups through their cell phones. An important concern here is that portable clients need security of their group information which ought not to be available to other group clients. To illuminate this issue, ABE or Attribute Based Encryption systems are utilized as they are limitlessly perceived as a substantial and strong component to give fine control over the information to authentic clients. In the meantime, as there are complex calculations included in key issuing and information encryption by AAs' (Attribute Authorities) and unscrambling by legitimate clients, there exists some efficiency's issues. Rekeying assumes a major part in dynamic frameworks where hubs come-in and move-out. As renouncement of client rights obliges framework to secure information from moved out clients, rekeying must be done on the whole information set having a place with that characteristic clients in the group. However the expense of re-keying is another concern towards framework productivity which ought not to be remunerated with trade off on the information security. There are numerous research works carried out on the information security for web applications utilizing ABE however there are restricted studies on CP-ABE in versatile processing with multi-power information stockpiling framework. We execute a framework which permits client groups to enroll, CAs'(Certificate Authorities) to permit enlistments of Users and AAs and dole out open Keys, AAs to oversee qualities and repudiate use access with re-keying and a concentrated server for information diligence. Trial results demonstrate the adequacy of proposed arrangement and proficiency of re-keying mechanism while bringing out clients access rights on framework structural planning.
4.5.2 Experimental Setup

To conduct the experiment two frameworks were created. Initial, an android based application for client enrolment, sign-in, transferring and downloading the information. Secondly, we built up an online application which has various modules, for example, Certificate Authority (CA), Attribute Authority (AA) and centralized cloud storage server. CA and AAs need to login in order to operate the framework, AAs and Users may send enrolment solicitation to CA for endorsement and designation of recognized ID and open key. Until and unless AA don't distribute ascribe to the client, client won't have the capacity to login to the framework. AAs may make any number of credits and have energy to disavow or change any quality for any specific client or entire group. For encryption and decoding AES calculation is utilized as it is turned out to be of higher security trust.

Android application utilizes HTTP web-administration for server connection and JSON items are utilized for information tying and transmission over server to application.

4.5.3 Android App Screens
4.5.4 Results

Figure 46: File Uploading Time
Figure 47: Rekeying Time

Figure 48: Registration ID & PK Generation Time
These results are produced for a constant framework created utilizing j2ee and android programming. The delays are ascertained automatically and are liable to shift as the gadget execution to minor extent.

Above results show different situations where delay is measured. Figure 49 demonstrates the time taken for generation of enrolment ID and open key for distinctive number of clients at the same time. Figure 50 demonstrates the transferring time of records of distinctive sizes. This measure is done to evaluate the deferral in transfer, encryption and db upgrade process. Figure 51 demonstrates the rekeying time for diverse number of documents stored on server. As denial includes keying of documents with new attribute so no. of documents get decode and encode costs little delay on server operation. Finally Figure 52 demonstrates the attribute assignment time for clients. All the more number of credits doled out to a client will have additional time delays in extent as one and only attribute can be doled out at once to the client. These outcomes demonstrate the proficiency of framework as every kind of operation take almost no time which is figured in milliseconds.

4.5.5 Discussion

This experiment focuses on giving versatile and all around sorted out application arrangement which takes after CP-ABE plan on mobile cloud storage. The proposed system gives a safe and effective solution for attribute revoking issues and
offers fine-grained access to genuine clients. The framework bolsters multi-authority CP-ABE plan where different AAs may exist to give clients more accessibility and adaptability to utilize the framework. The advantage here is the computation cost is imperceptibly decreased because of the circulation of work load among various elements. It is safe to outsource information on incredulous servers too because of better control and security. This proposed mechanism can be connected on different online social groups or business applications which permit clients to shape groups and offer file sharing within the group.