Mobile Cloud Computing and Data Masking Technique

[1]Mario Infant Raj P, [2]Vatchala B
[1] Research scholar, [2] Assistant Professor
[1] *Department of Computer Science, Prist Deemed to be University*
[2]*Department of Computer Science, Prist Deemed to be University*
[1] marioinfantraj@gmail.com
[2] Vatchala2020@gmail.com

***Abstract*— Mobile cloud computing the migration of the mobile applications to any operating system platform which can be user-friendly especially designed for mobile users which allows the users to use the applications and data's stored without being bound either to the operating system or the data storage capacity of the mobile. By this technique, the users can remotely access their applications and their data and the web portal using their unique id. It enhances the bandwidth coverage and better connectivity Cloud-based mobile apps more capable than any smart-phone especially the storage space Cloud apps' server-based computing infrastructure that is accessible through the mobile interface of an app Advanced technologies like Hyper-Visor virtual machines for smart-phones, cloudlets and Web 4.0, etc are contributing a lot toward MCC's rising popularity. Smart-phones have enabled us with 24/7 access to business applications and other collaborative services have upped the scope to increase productivity from anywhere, at any given time.**

Keyword: - **Cloud computing, key generation, data privacy, software as service, data encryption.**

I. INTRODUCTION

Cloud computing utilize the computing resource (hardware and software) that delivers as a service through a network (typically the internet) [1]. Cloud computing entrusts remote services with a user's data, software, and computation. Cloud computing aims to apply conventional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform trillions of computation per second[1]. The cloud computing uses a network of a large group of a server typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. Mostly, virtualization techniques are used to maximize the power of cloud computing.

The architecture for providing computing services through internet and access on-demand services and share network storage services and application. Cloud technology is in fully internet-based technique in which client data is stored with a data center like Google, Amazon(AWS).

1.1 Advantages of mobile cloud computing

- Reduces the cost and saves money.
- Increase the storage and maintain data confidentiality.
- Keeps software up-to-date and highly flexible.

II. ORIGIN OF THE RESEARCH PROBLEM

In daily life, mobile plays a vital role. The users face troubles like loss of contacts, photos, videos and digital data's because of the viruses, operating system upgrading patches and loss of mobiles and device upgrades[2].

To overcome these problems without loss of data and to protect and deliver safe data mobile-based cloud computing is required. And this can also sort out draining of battery life in mobile devices [3].

Usually, because of storing large data's in mobile devices such as documents, videos, and other resources mobile get overheated and battery life decreases. The continuous problem leads to decreases in the performance of mobile and hardware faults.

III. OBJECTIVES OF PROPOSED MODEL

- Providing facility software service with cloud computing.
- App-based methods.
- Providing backups.
- Offering suggestion.

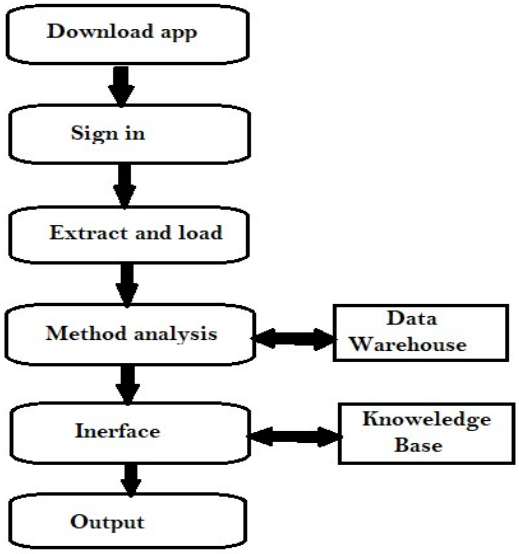

Figure1: Workflow of the proposed model

The figure1 shows the workflow of the model where user can register, sign in, upload and download all the data's from the data warehouse which is stored in the cloud. This model also uses the concept of a knowledge-base system with an interface engine, software's, and KVS with artificial intelligence. It also includes preserving privacy for the data stored in the cloud-based app. It allows encryption to data stored in the cloud and prevents phishing using visual cryptography[4].

3.1 Software As Service (SaaS)

It's the layer provider in which the client is ready to use application running on the infrastructure provider. The application service provider(ASP) provide different software application over the internet[8]. It enables the client to eliminate and install applications on his own.

The user can also increase or decrease the random access memory(RAM), processor cores, storage and change the operating system virtually without loss of data. These facilities are provided like a virtual machine (VM-ware, oracle virtual machine)[9]. The client should understand the data encryption methods which are applied to the data.

The client needs to be aware of how to secure data as defined in their data classifications, this to be handled in general and configuring options. The provider manages access to get the application, including security, availability, and performance.

3.1.1 Benefits of SaaS

- It helps to manage software from a central location.
- The user can sign up and quickly start using ingenious
- Software delivered in a one to many models
- No setup cost with SaaS, hence they are available in other applications

3.2 Platform As A Service (Paas):

Its is the middle layer which provides platform-oriented service. In this model, the client does not control the underlying cloud infrastructure including networks, servers, operating system and storage, the control is deployed by the applications and hosting environment Google app engine is the best for executing web application over the internet[10].

3.2.1 Benefits Of PaaS:

- Integrating web services via common standards.
- Reduces complexity.
- Makes development possible for non-experts.

3.3 Infrastructure As A Service(IaaS)

Simply this model is referred to as 'pay as you' go model can be utilized by co-operating and big scale industries for cost-effective and expense managing, it enables virtualization and cost-effective hardware

3.3.1 Benefits of IaaS:

- Supports big infrastructure scales on-demand to support workload
- Flexible and innovative
- Cost-saving in hardware
- Physical security of data center locations

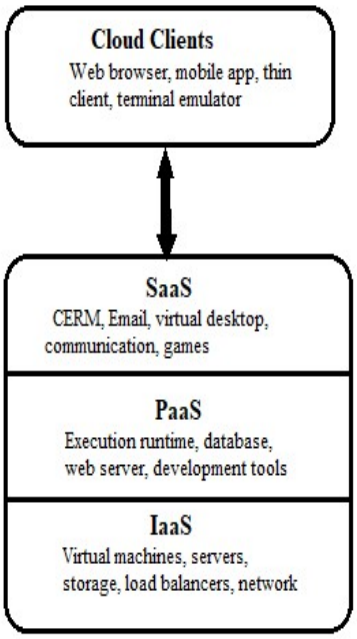

Figure3. Benefits of PaaS

IV. KEY GENERATION

This module used to generate the secret key by using the key generation algorithm and will send to the personal mail is of the user[5]. The secret key is a must for uploading and download files on the cloud server.

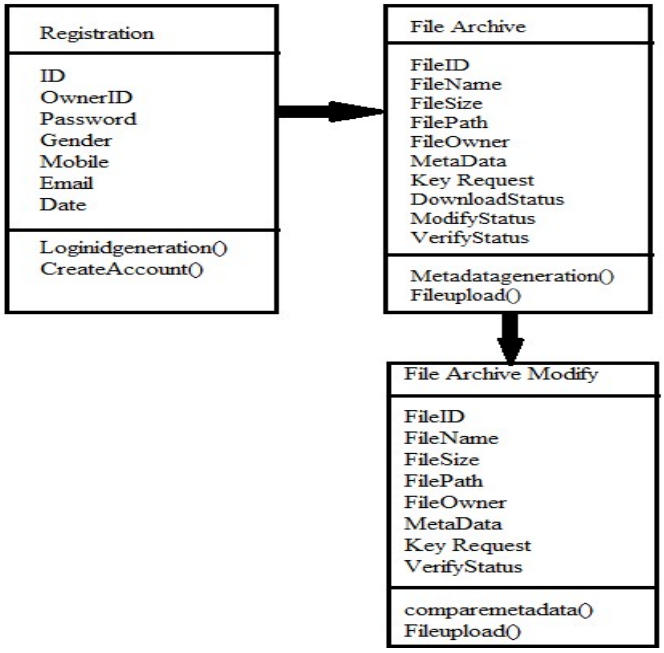

Figure3. Class Diagram

V. DATA PRIVACY

Data privacy in the cloud plays a major role both for the cloud provider and user with a large amount of data which is stored at an increasing rate. Our traditional data storage system will not able to handle data and becomes a challenge[11]. The attacks focused on data mining while storing the data is very sensitive. This model prevents intermediate data leakage with encryption and decryption concepts.

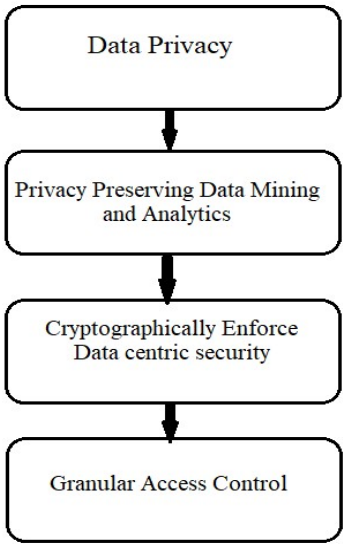

Figure4: Block Diagram of Data Privacy

VI. DATA ENCRYPTION

The prescribed data mining and cloud use homographic encryption as well as the RSA algorithm to enhance the security of the data mined in the cloud. The system ensures data security to assure data backup and retrieval. It preserves security confidently and obtains data privacy[6]. The data-based are mined on the cloud-based on homographic encryption which allows the encrypted data to be arbitrarily computed. This encryption also provides with two types of data masking

- Static data masking which is used by most of the organizations for sensitive data protection
- Dynamic data masking(DDM) where the strategy of controlling or limiting unauthorized access to the data

These data masking techniques also use techniques like substitution, shuffling and encryption

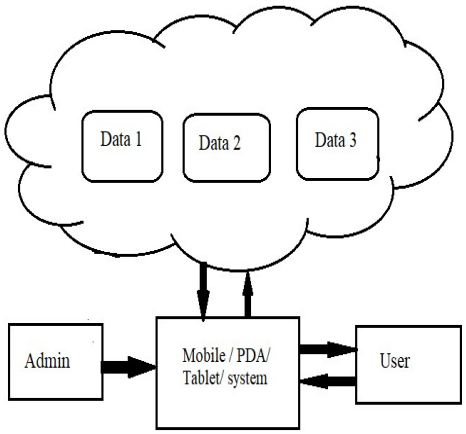

Figure 5: System Architecture of sender and receiver Side

6.1 Data Security In Cloud

6.1.1 Sender side

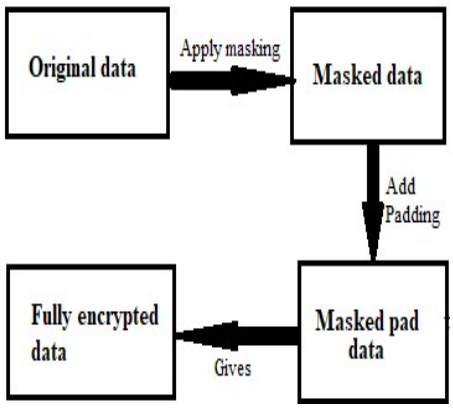

Figure6: Sender side

The encryption process usually takes place on the socket layer of the sender side. After masking the masked data is applied with the padding and much more secure than before[12]. It makes double encryption and securely transfers to the receiver.

6.1.2 Receiver Side

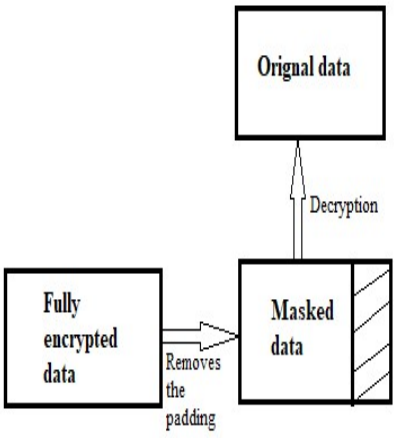

Figure 7: Receiver side

At the receiver side, reverse the process of the sender occurs[12]. The data which is double encrypted is being decrypted doubly. At the first level, the padding of data is removed and after we get the masked data. Now the mask of the data is removed to obtain the original data[13].

VII. WORKING PRINCIPLE

The user fetches the data from the server and installs it on his device and opens and registers the app and selects the server location and confirms the basic details. Then he sends a key request by selecting the app's he uses frequently and fetches it inside the app. Using single cryptographic key he logs into all the app's the data stored in the device automatically using the internet uploads to the cloud. This makes sure the user to be hassle-free for data being lost.

The application opens like a virtual machine like Oracle virtual machine and Vmware where the user can select the memory, random access memory, operating system and proceeds to the next level. It is very user-friendly as the in-built application has preloaded operating system so it is easy to switch over across OS platforms like android, windows, Linux, iOS, and blackberry. The user did not need to restore the purchase either reinstall the applications when switching the OS platform.

The user enjoys the data which was previously stored as it is in the switched operating system also. This gives the benefit and makes a boon to the user to be hassle-free while the loss of mobile, theft of phone or crash of operating system and any damages so the user can enjoy full fletched freedom of being locked on same devices and can move on frequently within minutes to a new device[16].

The integration of all app's in a single app decreases the mobile memory, occupies a small space and increase battery life this can also integrate with E-Sim concept and allows the user to track locate and enhances the security, safer contacts, save messages and texts. This will be a greater boon to the upcoming generation.

VIII. CONCULSION

This paper present mobile cloud computing and data masking technique. We implement the mobile cloud computing on Amazon(AWS) elastic cloud and Google as a data center. We also implement a benchmark to evaluate the performance of mobile cloud computing and the data masking by testing the scalability and integration. From the design and evaluation result, we summarize potential risks and benefits to moving data to mobile cloud and data masking. This summary could help the cloud developers to migrate the data and existing applications quickly and safely on the Google data server and Amazon(AWS)

IX. REFERENCES

[1]. Sneha Sakharkar, Shubhangi Karnuke, Snehal Doifode, Vaishnavi Deshmukh, “A Research Homomorphic Encryption Scheme To Secure Data Mining In Cloud Computing For Banking System”. IJSRSET volume 4, Issue 4, March 2018.

[2]. Dharma P. Agrawal, Brij B. Gupta, Shingo Yamaguchi, and Konstantinos E. Psannis, “ Recent Advances in Mobile Cloud Computing”. Article ID 5895817, February 2018

[3]. Dr. Birajkumar V. Patel, Dr. Dipti B. Shah Implementation of Cloud Computing (Software as a Service) for Product based Search Engine. IJSRST volume 4, Issue 2, February 2018.

[4]. Geethamani G. S, Ranjani S, Preserving Privacy In Public Auditing For Data Storage Security In Cloud Computing. IJSRCSEIT Volume 3, Issue 1, February 2018.

[5].R.Manikandasamy”Remote Desktop Connection Using Mobile Phone ”International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 8, August 2013.

[6]. Remote Control of Mobile Devices in Android Platform Angel, Gonzalez Villan, Student Member, IEEE and JosepJorbaEsteve, Member, IEEE.

[7]. Everette E. Adam, Jr. Ronald J. Ebert; Production and Operations Management, Fifth Edition, PHI Learning Private Limited (2012)

[8]. James A. O'Brien; Management Information Systems, Fourth Edition, Galgotia Publications Pvt. Ltd (2001)

[9]. Deepti Mittal, Damandeep Kaur, Ashish Aggarwal, "Secure Data Mining in Cloud using Homomorphic Encryption". IEEE Cloud Security.

[10]. SunandaRavindran, ParsiKalpana, "Data storage security using partially homomorphic Encryption in cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4.

[11]. Hemalatha, Dr. R. Manickachezian, "Performance of ring-based fully homomorphic Encryption for securing data in cloud computing", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 11, November 2014.

[12]. Priya Dhir, Sushil Garg “Survey on Cloud Computing and Data Masking Techniques” International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 6, Issue 4 April 2017

[13]. Data Masking: What You Need to Know What You Need To Know Before You Begin A Net 2000 Ltd. White Paper.

[14]. Swot Analysis of Mobile Cloud Computing A.M.S.Zunaitha Sulthana*, L.Clara Mary*, A.SangeethaDepartment of computer science, MIET Institution, Trichy

[15]. A Survey on Recent Trends, Process and Development in Data Masking for Testing Ravikumar G K1, Manjunath T N2, Ravindra S Hegadi3, Umesh I M4

[16]. Data Sanitization TechniquesA Net 2000 Ltd. White Paper