Juni Khyat
(UGC Care Group I Listed Journal)
ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

SURVEY ON SECURITY CHALLENGES AND ITS SOLUTION ON MOBILE CLOUD COMPUTING

Vikram Patalbansi[1] Dr. G. Prasnna Laxmi[2]
[1]Research Scholar
Pacific University, Udaipur India
[2]WOS – A Program(DST)
Andhra University
[1]Email : vikrampatalbansi14@gmail.com
9619455631
[2]Email : prassanalaxmigandi@gmail.com
7021997415

ABSTRACT: Mobile Cloud Computing (MCC) is the combination of two technologies like Mobile Computing and Cloud Computing which are the main hot topics in recent industries business world. It's market are growing rapidly since 2009 when use of smartphone and mobile devices are became popular. In this paper we are going to review different types of security challenges and it's solutions. And also going to analyses the infrastructure of MCC and it's future research trends. As per different running Mobile Application on Mobile Devices scenario, we are going to analysis different privacy and security threat as Security as a Service (SecaaS) in different scenarios and practices based on the requirement of individual applications like mobile threat and cloud threat. Apart from this we are going to review in heterogeneity in MCC during Data Transmission in wired and wireless networks.

Index Term: Mobile Cloud Computing, Security issues, SecaaS, Interoperability and Portability in mobile network.

1. INTRODUCTION

Cloud computing is new generation technology that consists of networking, distributed computing and database management system , that provides on-demand to access shared pool of configurable resources on a pay per use basis. According to National Institute of Standard and Technology,USA [1] definition from September ,2011 released in its "Special Publication 800-145" Cloud Computing is define as :

"Cloud Computing is a model for enabling convenient on-demand network access to a shared pool of configurable resources (e.g. networks , servers, storage , application and services) that can rapidly be provisioned and released with minimal management effort or service provider interaction."

[2]Cloud Computing gives the functionality regarding in computing like Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). With the help of this functional model user can get utility from cloud computing to increase their capacity and capability dynamically without investing in new infrastructure, training new personnel, licensing new software etc.

However the vast increase use of Smartphones and laptop in computing, the actual realization is observed how to access the cloud functionalities from Mobile devices irrespective of its lots of challenges like battery life, limited storage and display and less processing power and bandwidth problems in mobile communication. The combination of Mobile Computing and Cloud Computing is known as Mobile Cloud Computing (MCC). It refers to uses of cloud computing through mobile devices with help of its various mobile applications. The mobile application with the help of mobile network and cloud computing provides optimal service to mobile user through internet where resources are exits at remote location.

[10]Security is a major challenge in Mobile Cloud Computing because very persons in IT business prefer to store their personal data in Cloud Data Centre to minimize store cost. Data or information are stored in centralised location so there are chances of stolen of data by hackers. As well protection is needed during transmission of data from data centre to mobile devices in wireless communication. To achieve this we have lots of challenges likes data fragmentation & integration over data transformation with proper format, bandwidth and security of signal during wireless transmission from mobile device to cloud server and technologies threat like hardware related threats and software related threats as well .Storage Networking Industry Association proposed the theory of Cloud Data Management Interface (CDMI) for protecting or securing the data over cloud data centre. The CDMI standardization developed by Storage Networking Industry Association. CDMI allows users to tag the data with special metadata. The metadata can be used to code services that must be provided such as encryption, back up, deduplication, replication, compression archiving etc. The services increase the value of user data existing in the cloud. Cloud Data Management Interface (CDMI) is the first industry developed standard for cloud data was

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

created by SNIA Cloud Storage Technical Work Group. By implementing a well-documented standard interface , user can freely move the data from one cloud vendor to another without the problem of conforming or adjusting to different interface. It include a common inter – operable data storage format for safely moving data and its requirement from one cloud provider to another.

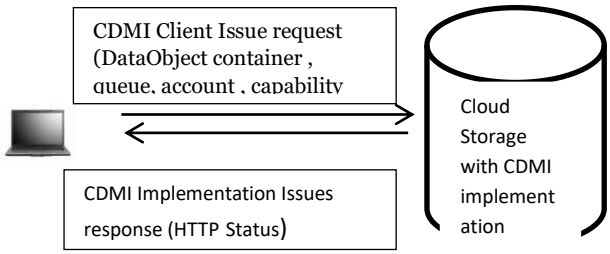

Fig.1 Schematic diagram for Cloud Data Management Interface.

2. OVERVIEW OF MOBILE CLOUD COMPUTING

Mobile Cloud Computing is one of the kind of network architecture where data processing and storage can happen outside the mobile devices. As we know that all kind of electronics mobile devices does not need to have large storage capacity and powerful CPU speed. All data processing are happen outside the mobile devices on a centralized computing platform located in clouds. Now any users does not need to invest lot of capital as well as resources because they can share or access data from the cloud. The operating system on mobile devices can not having more importance because through mobile, cloud computing application can be access via browser. Apart from this ,there are some issues in using MCC like bandwidth , access scheme, security etc.

A. Mobile Computing

Today there are lots of development in Mobile Devices such as smart phones, PDA ,GPS Navigation and laptops with variety of mobile computing , networking and security technologies. Hence any mobile devices can be connected to any wireless network like Wi-Fi, WiMAX, Ad Hoc network with changing it's basic hardware configuration. Due to its movability, mobile nodes in mobile computing network can establishes connection with others even fixed nodes in wired network through Mobile Support Station (MSS) during their moving.

But during establishing the connection, there are frequent disconnection and inconsistency because of limitation in battery power, charge of wireless communication, network condition and son on passively or actively. Due to wireless signals are susceptible to interference and snooping, the MSS in mobile computing faces various security issues like signal disturbance, security, hand off delay, limited power , low computing ability etc.

In this paper we are going to focus on efficient and effective management of issues and challenges pertaining to security and privacy in mobile cloud environment through set of recommendations and best practices on the top of work done by various researches in their paper.

The paper is organized as follows. Section two presents background and related works by other researchers. The issues and challenges in privacy and security of mobile cloud computing framework are presented in section three. The primary considerations of SecaaS are listed in section four with different scenario and practices. Section five presents our recommendations and best practices adopted for mobile cloud computing in ensuring adequate security and privacy measures. Finally, section six concludes with way forward for future work.

3. BACKGROUND AND RELATED WORK

Prof. Han Q. and Prof. Abdullah Gani [3]from University of Malaya has stated that Mobile Cloud Computing (MCC) is combination of Mobile Computing and Cloud Computing and analyses the features and infrastructure of MCC. Using the MCC architectures studies they derive some challenges and research issues. The major challenges come from the characteristics of Mobile Devices and quality of Wireless Communication Networks. The limitations of Mobile Devices like storage space, size of Screen, wireless sensing technology and operating system platform. To overcome these problems we have to consistently develop mobile computing programming so that virtualization of mobile screen images and distribution of task can be done on various machines of cloud network. For these we have to develop optimal strategy and algorithm how to divide the task so that which task run on cloud and which task run on Mobile.

a) Upgrade the bandwidth of wireless communication and make regional data centers to fetch information speedily.

b) To avoid various load on Mobile devices, use virtualization technique to generate the clone of mobile processing images on TPA.

Debasis Bandyopadhyay and Debasis Jana[4] both senior member of IEEE and by profession both are software consultant stated the some security threat and it's measures for Mobile Cloud Computing. Some of the threats and their solutions are suggested are as follows.

a. Loss of Mobile Device.

If Mobile is lost and theft, there are chances of misuse of information. Hence in MCC each and very devices are connected to centralized authentication and security center. And also suggest to keep control over data by proposing Secure Multiparty Computation (SMC) done with help of Virtual Private

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

Network (VPN) router and nodes. So no single host does not have capability to process the data which having encryption and use multiple secret shared database. This technique also known as Homomorphic encryption. In these no single host alone cannot recover the original data.

[5] Zohreh Sanaei, *Member, IEEE,* Saeid Abolfazli, *Member, IEEE,* Abdullah Gani, *Senior Member, IEEE* and Rajkumar Buyya, *Senior Member, IEEE* propose the theory of heterogeneous cloud resources accessibility network environment dividing it into two dimension viz. horizontal and vertical. In this paper they show the interpretability among MCC application and code fragmentation to develop cross platform mobile application. They also shows the challenges and their solution. Due to various heterogeneity of various mobile network and dimension and device features can effect overall performance of the remote processing of MCC. For this we have lots of research challenges among heterogeneity in MCC.

[6] D. Popa , Technical University of Cluj-Napoca,Communication Department,Cluj-Napoca Romania ,Daniela.poa@com.utcluj.ro and , K. Boudaoud University of Nice Sophia Antipolis , M. Cremene , M. Borda [4] proposed the their research theory in paper Overview on Mobile Cloud Computing Security issues that there are two types of threat in Mobile Cloud Computing one is Mobile Threat and another one Cloud Threat.

Generally Mobile Threat based on Hardware and Software. On this basis mobile threat are divided into several categories such as : application based attack, web based attack , network based attack and physical based attack. Application Based attack should be performed either offline or online with help of malware or spyware software. Web based attack can performed online with help of phishing scams,driven-by-downloads or browser exploits. In addition to his different technique are also used to obtain private data like repackaging of in built mobile App and misleading disclosure and update. But in case of Cloud Threat, security issue have been classified in terms of different concerns like domain concerns , services concerns , actors concerns and properties concerns. In Domain concerns we have issue like data ownership and data location rules and regulations. In operation domain we have challenges like security in storage of data and transmission of data between cloud and mobile over wireless network and data access and integrity, data loss , unsecured applications and interfaces ,denial of services. In case of Actor domain , the malicious client or software are exist into the cloud data center. This may cause that outsider may listen to the network traffic or it may insert malicious traffic and launch the denial of service attack.

[11]Prof. Al-kindy Athman Abdalla and Prof. Al-Sakib Khan Pathan from International Islamic University Malaysia, Kuala Lumpur has propose some security measures during transmission of data between Mobile Devices and Cloud Data Center. They propose the theory that some commercial cloud storage services protect users' data located in server-storages by introducing client based or server-based data encryption. When client based encryption is used, it is ensured that the user's data are encrypted before transmitting to the server. All components related to encryption, such as encryption process, library and data keys, are hosted by the client program. By using these components, the client program generates a one-time-use symmetric key for data encryption. This key will be encrypted using the user's asymmetric public key and uploaded with encrypted data to the server. When the user wants to download his or her data, the client program requests this encrypted data key along with data and then decrypts the data key using user's private key and finally decrypts the data. But during mobile client and data centre server communication they failed to propose theory that how we fragments the large amount of data into small chunks so that it can transmitted over wireless network and store over various location to avoid eavesdropping by hackers. This creates lots of challenges like i) Runtime Issue (to make our data compatible to various cloud environments) ii) Redundancy issue (over wireless transmission due to various impairment like fading multiple copies of data will generates) iii) Implementation issues (to secure data we have to apply various encryption algorithm)

[12] Amin Subandi, Rini Meiyanti, Cut Lika Mestika Sandy, Rahmat Widia Sembiring from *Universitas Sumatera Utara", Medan, 20155, Indonesia proposed theory of three - pass protocol* a framework that allows a party may send a message encrypted securely to the other party without having provided the key. This Three-Pass protocol invented by Adi Shamer about 1980 in applying Three-Pass protocol does not always have to use a cryptographic algorithm, because basically, this technique has its own function, namely to use the function exclusive-OR (XOR) . In this research they were analyze the possibility of security on the integrity and confidentiality might be better to implement a three-pass scheme protocol during the process of sending and receiving messages using XOR function of the message is used as an example of an experiment by changing the message into an array of binary numbers.

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

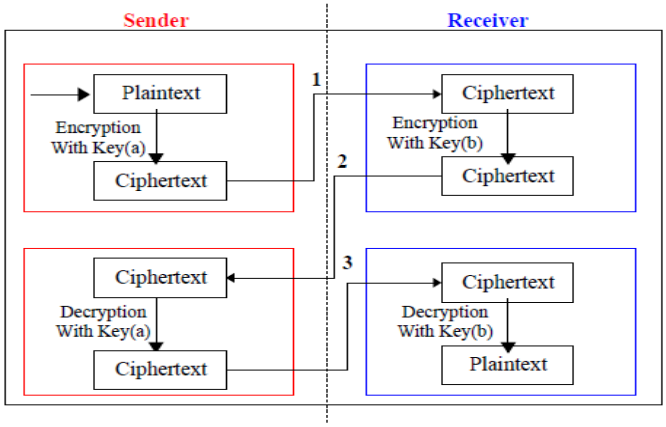

Fig.2 Schematic Representation of Three – Pass Protocol

[13] For example assume mathematical problem from research paper "Study of Three Pass Protocol on Data Security" by Robbi Rahim , Ali Ikhwan from Universitas Pembangunan Panca Budi, Jl. Jend. GatotSubroto Km. 4,5SeiSikambing, 20122, Medan, Sumatera Utara, Indonesia as follows

Three pass protocol process on the sender and receiver use each key and requires no key exchange. To test the three pass protocol scheme can be seen in the following example:

Plaintext = A

Binary = 01000001

Here are three pass protocol process of the plaintext

01000001 -> plaintext

01010101 -> Key of A (Ka) Keywords Sender

00010100 -> Send To Recipient ciphertext (C1)

11010101 ->Key B (Kb) Lock Receiver

- 11000001 -> ciphertext Send To Sender (C2)

01010101-> Key A (Ka)

10010100 -> ciphertext Send To Recipient (C3)

11010101 -> Key B (Kb) Lock Receiver

01000001 -> plaintext

Looks plaintext transmitted and received by the appropriate shipping and respectively do not need to know the key of the encryption and decryption enough to use a key.

01000001 -> plaintext

01010101 -> Key of A (Ka) Keywords Sender

00010100 -> Send To Recipient ciphertext (C1)

11010101 -> Lock B (Kb) Lock Receiver

11000001 -> ciphertext Send To Sender (C2)

01010101-> Key A (Ka)

10010100 -> ciphertext Send To Recipient (C3)

11010101 -> Lock B (Kb) Lock Receiver

01000001 -> plaintext

Encryption and decryption process over if done by cryptanalyst XOR technique to get the C1, C2 and C3 it can be seen the original message, with the following process

00010100 -> ciphertext C1

11000001 -> ciphertext C2

11010101 -> XOR C1 C2

10010100 -> ciphertext C3

01000001 -> plaintext

But main disadvantages of this system is that we have limited encryption key combination to generate cipher text. There is less chances of generating same cipher text by using same encrypting key but it may happen randomly any time. So code redundancy will happen in this scenarios. Hence some new theory or algorithm will have to develop to avoid code repetition.

[14] Monjur Ahmed and Alan T. Litchfield from Auckland University of Technology, Auckland, New Zealand were proposed the theory of Taxonomy for Identification of Security Issues in Cloud Computing Environments in their research papers. On the basis of studying various case studies on corporate cloud system they drive the two kinds of factors involves in security threat of cloud data.

First one is Human Threat and Second one is Technological Threat. Here we study only Technological Threat. Technological Factors threats having two types 1) hardware-related threats that relate to the Cloud infrastructure and network, and (2) software-related threats that relate to platform and application resources above the Cloud infrastructure. To overcome above two threats we have to develop proper network configuration so that information stored in distributed manner. If anyone wants to access full-fledged information then he has to go through different node over network and authentication must be done at every node. For this purpose they did not mentioned proper network algorithm to trace valid information. In case of software related threats we have different scenarios. On Cloud Data centre we have one specific operating system and application software to manage information. Different mobile user having different operating system and application based software. To make proper standardization of software or compatibility to different mobile hardware or software proper security guidelines we have to develop. For this purpose we have to do further research on platform independent software tools and their security measures depends upon software configuration.

[15] KashifMunir and Lawan A. Mohammed University of Hafr Al Batin, KSA proposed the their

research theory in paper SECURE THIRD PARTY AUDITOR (TPA) FOR ENSURING DATA INTEGRITY IN FOG COMPUTING that protocol to ensure data integrity which is best suited for fog computing environment. Fog Computing is extended version of Cloud Computing. It is a decentralized computing and it is a highly virtualized platform which provides computation, storage, and networking services between IoT devices and traditional cloud servers.

They propose the theory of PDP (Provable Data Possession) model for verifying if an untrusted server stores a client's data. The data owner processes the data file to generate some metadata to store it locally. The file is then sent to be stored in the server, and the owner may delete the local copy of the file. Clients may encrypt the file earlier to upload it to the storage. After that, the client asks the server to reduce a proof of the stored file for security concern.

The main drawback of this theory is that whole files are encrypted at one instance, hence long time to reply to client and in between this connection may break and proper authentication reply does not send to original client. And for verification or authentication, we have to retrieve total file which leads to extra usage of internet or network bandwidth.

Hence to overcome above challenges, we have to encrypted small size data for faster processing. To achieve this we have to generate the algorithm to task or file slicing for encryption. Assign sequential order for each and every distribute of file parts. And during transmission for parts of file to server by mobile client we have to convert it into network compatible format. And use the concept of Spread Spectrum technique use in wireless communication for encrypting the file information. But pseudo code or key length must be standardized like 128 bits ,196 bits or 256 bits. Longer key more complicated in encrypting the information.

[16] Mr. Dalila Slimania, Fatiha Merazkaa from *LISIC Lab, Telecommunications Department, USTHB University, Algeria proposed the theory for generating the pseudo code for encrypting the cloud data whenever digital data stored or processed by any Mobile electronic devices gets converted into analog signal to send information to Cloud Data Centre or Server.*

In this paper, they proposed an encryption system for speech signals based on circular shifts in row and column. This cryptosystem uses three secret keys. The original key is generated, randomly, using a pseudo noise sequence generator, and the two other keys are obtained by using the main key. The encryption system also uses Discrete Cosine Transform (DCT) or the Discrete Sine Transform (DST) to remove the signal intelligibility. They explain this encryption technique as follows.

Algorithm 1 ENCRYPTION ALGORITHM

• Step 1: Framing and reshaping into 2-D block
• Step 2 : Circular shifts (in row and column)

1st Round

• Step 3 : Generation the main key K1
• Step 4 : Permutation with a main key K1
• Step 5 : Generation of the mask M1
• Step 6 : addition of mask M1 •

2nd Round

• Step 7: Discrete Cosine Transform (DCT) or Discrete Sine Transform (DST)
• Step 8 : Generation of second key K2
• Step 9 : Permutation with a second key K2
• Step 10 : Generation of the mask M2
• Step 11 : addition of mask M2 •

3rd Round

• Step 12 : Inverse Discrete Cosine Transform (IDCT) or Inverse Discrete Sine Transform (IDST)
• Step 13 : Generation of third key K3
• Step 14 : Permutation with a third key K3
• Step 15 : Reshaping into 1-D format

The above algorithm can be diagrammatically can be illustrated as below.

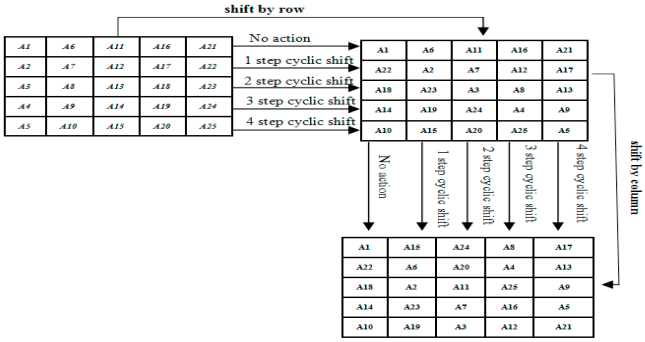

Fig. 3 Circular shift by row and column

Round 1: - Generation of secret keys

The encryption algorithm uses three secret keys:

•The original key is generated, randomly, using a pseudo noise sequence generator.
•The second key is the inverse of the original key.
•The third key is generated from the original key by dividing it into two halves and reversing the two halves.

For example:

If K1 represent the original key :K1=00110001

The second key K2 is obtained by inversing K1 :K2=11001110

The third key K3 is generated from K1:K3=00010011

Permutation with a secret key

They use a circular shift by row and column for permutation process.

The secret keys control the permutation process:

1) If the key bit is 1:the row or column is shifted by (index of row or column-1) steps.
2) If the key bit is equal to 0: the row or column remains unchanged.

Figure below show an example of permutation with secret key by row and column.

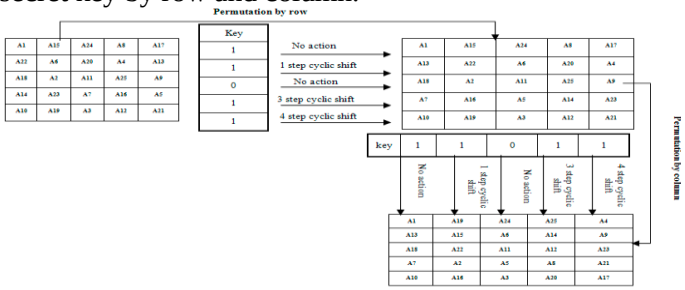

Fig. 4 Row and column permutation steps

Generation of mask

The encryption algorithm uses two masks M1 and M2 which are respectively generated using a circular shift of the keys K1 and K2.

Figure 5 show an example to generation of mask.

The application of masks M1 and M2 are used to encrypt non permuted portions of the signal to increase the security of the crypto system.

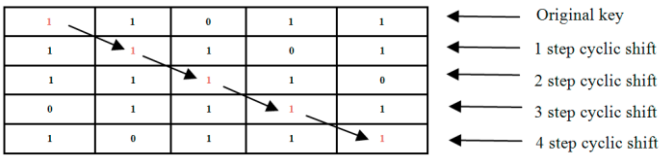

Fig. 5. Generation of mask Addition of mask

The mask generated from the encryption key is then added to the block. Thereafter, we use the subtraction of 2 for any value greater than 1.

Round 3

Discrete Cosine Transform (DCT) or Discrete Sine Transform (DST)

To remove the intelligibility of speech signal, we used the Discrete Cosine Trans-form (DCT) or the Discrete Sine Transform (DST) after applying the mask.

At the receiving end we have to follows following decryption algorithm.

Proposed Decryption Algorithm

The decryption algorithm uses inverse operations to encrypted message to retrieve the original message.

Decrypt the encrypted analog signal at data centre as the following steps:

Algorithm 2:- DECRYPTIONALGORITHM

•Step1:GenerationofthreesecretkeysK1,K2 and K3

Step2:Framing and reshaping into 2- D block

•Step3:Inverse permutation with a third key K3

•Step4:Discrete Cosine Transform(DCT) or Discrete Sine Transform(DST)

•Step5:Generation of the mask M2

•Step6:Subtraction of mask M2

•Step7:Inverse permutation with the second key K2

•Step8:inverse Discrete Cosine Transform(IDST) or inverse Discrete Sine Transform(IDCT)

•Step9:Generation of the mask M1

•Step10:Subtraction of mask M1

•Step11:Inverse permutation with the main key K1

•Step12:Inverse Circular shifts(in row and column)

•Step13:Reshaping into1-D format.

In the decryption process,we used the subtraction between the block and the mask and the addition of 2 for any value below-1 to guarantee the correct reconstruction of these sample values.

In the next paper We will simulate above algorithm using MATLAB and NS – 3 simulator to draw the valid graphical representation of transmission working between mobile and cloud data centre or server.

Till now we see all the proposed security theory are applicable to user to avoid any malicious attacks. But whenever mobile user stored the their data into cloud storage or data centre then this data are secure to outside user but cloud owner and administrators can view and use these information without knowledge of actual owner. Hence there is need to protect our data over cloud storage from cloud service providers and administrator. [15] Mr. Hassan Reza and Ms. Madhuri Sonawane from School of Aerospace Sciences, Department of Computer Science, University of North Dakota,Grand Forks, ND, USA proposed the theory for of security mechanisms to prevent unauthorized access by unauthorized user by the cloud administration in their research article Enhancing Mobile Cloud Computing Security Using Steganography. In this paper, they demonstrate how steganography, which is a secrecy method to hide information, can be used to enhance the security and privacy of data (images) maintained on the cloud by mobile applications to encrypt their data from unauthorised access by cloud administrator. .

Using this model, they show how to works with a key, which is embedded in the image along with the data, to provide an additional layer of security, namely, confidentiality of data. In the steganography method user encrypted their information into some image or some other hidden representation format like data and transfer to cloud storage. Hence this information can be interpreted to mobile user only. Due to secret representational format, cloud administrator cannot be interpreted anyway.

Whenever cloud storage or data centre wants to process particular user information then cloud administrator cannot process without consult with mobile user. He demands secret key from mobile user and after getting key , information gets decrypted and process and send to user or store at cloud storage. But using this theory mobile user can encrypts the small amount of information but in case of bulk amount of

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

data this procedure is hard to implements. Mr. Hassan Reza and Ms. Madhuri Sonawane does not proposed the theory or algorithm that how to divide bulk information into small parts or slicing the information and task into smaller parts so that Steganography can be flexible to implements. In next paper we will try to proposed theory on algorithm for dividing the bulk task and information into small chunks and apply strong theory of security algorithm on task to keep way cloud administrator from viewing mobile user data on cloud storage.

4. ISSUES AND CHALLENGES OF MOBILE CLOUD COMPUTING

With reference to previous section, we are able to collect some major issues and challenges of MCC. In this section according to our study and look out, we are going categories these issues and challenges as follows

A. Data Security and Privacy Issues

[7] In MCC we have serious issues about data security in cloud computing during transmission of data and processing of data. Following points must take into consideration for data safety.

i. Data loss or unauthorized access.

ii. Privacy of data while storing and transmission of data through various modes.

iii. Generation and allotment of encryptions and decryption keys.

iv. Security and auditing issues of hardware machine at cloud data center and mobile devices

v. Maintenance for consistency of software qualities and transmission media.

vi. Compatibilities issues in mobile application, mobile platform due to different vendor standardization.

A. **Open Issues and Future Research Directions**

[8] Although now a days MCC are widely used in industries as well as on social media through mobile devices with the help of different mobile software application and platform, still there are some challenges while implementing in practical use of MCC services. In short we are going enlist some points as follows.

i. Data delivery: Due to some technical and hardware restriction of mobile devices, problems in accessing the data through cloud can be solved using special application and middle-ware hardware.

ii. Task Division: Instead of accessing or processing bulk data or application at one instance, the researchers produces a theory for task division. Means which task run on Mobile and which task run on Cloud. But till now there are lacks of research in optimal strategy or algorithm on how to divide this task which one should be processed by cloud and which one by mobile devices. Also there are also research gaps found in optimization of task scheduling as well as allocation during transmission and processing

iii. Common standardization for interface and service delivery: As we know in MCC, all kinds of data accessing performed using mobile devices through web browser interface via internet. In market we have various vendors for web browser and mobile devices. So there are lots of compatibility issues among interface tools and mobile platform. To overcome this flaw, some research must be done to develop standard protocol and interface to make uniformity in MCC.

iv. Quality of services during transmission of data: The Original objectives of MCC are to provide PC-like services on mobile device. But data transmissions are happened only through wireless transmission in MCC between mobile devices and cloud data centers. So there are lots of challenges in data transmission like bandwidth limitation, network congestion and disconnection and signal attenuation and various wireless transmission impairments. Also there are lots of challenges in authentication of wireless signal in various wireless networks like Wi-Fi, WiMAX, Li-Fi, Cordless System etc. With respect to specific wireless network, we have to develop some common standardization and protocol for security.

B. **Classification of Security threats for Analyzing solutions.**

To maintain the user trust in MCC, we have to provides proper solutions to various challenges. As we know in medical science to heal any persons we have to diagnosis his problems and prescribe some medicine according to its health issue. Similarly to provide the solutions to Security threats in MCC, we have to bifurcate various security threats on this basis of locations and users. So Security Issues in Mobile Cloud Computing can be classified as follows: Mobile Threats and Cloud Threats.

i. Mobile Threats: As lots of use of Mobile devices such as Smartphones, so many mobile applications are installed in mobile devices to operate. Due to this various mobile attacks are performed like application based attacked, web based attacked, network based attacks and physical attacks.

In Application based attack we have various types Malware , Spyware , Phishing Scams, Drive by downloads and Repackaging of Mobile Application Software and Misleading disclosures.

ii. Cloud Threats: Over the Cloud Computing database, all user information's are centrally stored in Data Centers. So to provide the security to these data we have to develop some parameters or protocol. Before that we have to analyze the types of Cloud threats like domain concerns, services concerns, actors concerns and properties concerns.

2. PRACTICES AND SOLUTIONS USE IN MCC AS A SecaaS

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

[9] In MCC environment, different Cloud Service Provider (CSP) whether it was private cloud or public cloud provides different security solutions for different media like media, web, email, allied for prevention for data loss as well as robust identity and access management (IAM). For each cloud vendor it provides the different guidelines to adopt various standardization for each area of SecaaS. The important guidelines provided by Cloud Security Provider (CSP) for IAM SecaaS components are Authentication (Strong and Risk Based Authentication), Identity Federation Services (Federated Identity Management, Federated Single Sign-on) Identity Management Service (Provisioning and De-provisioning, Centralized Directory Services, Privileged User Management) Authorization, Access management, Audit and Reporting. Using these components CSP can performed the job of prevention of data loss, web security , business continuity planning(BCP) as well as disaster recovery(DR) , encryption , email security, security assessment, intrusion prevention and detection systems (IDS/IPS), security information and event management (SIEM).

With respect to above threats. in case of mobile devices lost user has to block or deactivate the devices. But to recover original data as usual on different devices we have to set some preventives measures like the physical storage should be encrypted and stored data must remain secured against unauthorized access even when it is lost or stolen. The device must be connected to a central security server on a periodic basis to scan and remove the PAI (Personal Account-holder Information).

In case of Information Leakage during socially access cloud data through internet, we have to provide some third party authentication (TPA) PIN validation or with the help of card validation.

Cross Site Access due to request forgery (CSRF), scripting (XSS) or non-terminated login sessions – Cross-site scripting (XSS) may try to inject vulnerable client-side script into web pages viewed by other users. So Cross site forgery can be protected with help of Payment Card Industry Data Security Standard (PCI DSS) compliance and Open Web Application Security Project (OWASP) guidelines to validate user supplied input to include unique token in a secreted field so that the value can be sent in the body of the HTTP request, while avoiding its inclusion in the URL, which is subject to direct exposure. All non-terminated sessions must be automatically signed out in timely manner

5. [9] RECOMMANDATIONS FOR EFFIEICENT AND EFFECTIVE PRIVACY AND SECURITY CONTROL

I. Proper Selection of computational task which will be proceeding on Cloud and another task will be on Mobile devices in accordance with mobile device capability.

II. Partition of computations for running on cloud between the mobile devices and the cloud environment - to reduce energy consumption while partially processing the real time data on the mobile devices

III. By providing multiparty encryption technique on data at various level with help of Secure Multiparty Computation (SMC) and Homomorphic Encryption (HE)

IV. During communication between mobile and cloud ,we have to provides various secure measures or guidelines at each very nodes during transmission of data. So during communication or transmission time data cannot be tamper. If tamper it can easily traced and can performed recovery operation.

V. [5] By implementing heterogeneity in MCC among mobile devices, cloud and wireless network to interoperate the functionality of each components to boost performance and security. In case of mobile devices we have various types of operating system or hardware configuration. So whatever mobile application are developed it should not runnable to other devices, Hence to make interoperability among mobile devices platform independent characteristics should develop among various devices. In case of cloud , cloud user forced to use similar cloud configuration irrespective of their information. Hence we have to provides different heterogeneity in Cloud Service Provider by implementing virtual machine standardization like Open Virtualization Format (OVF) and facilitate the deployment of virtual appliances in various clouds. In case of Wireless Network any changes in network technologies directly impacts the efficiency and effectiveness in performance of data during transmission of data if mobile devices continuously changing location. So some heterogeneity must be provided in wireless network.

6. Conclusion

At last in the above paper we proposed the theory on Mobile Cloud Computing in short to show some challenging security issues and some existing features and their solution with reference to various MCC framework. This framework gives us guidelines regarding user data privacy , data storage and energy preserving data sharing. To attend more proper security MCC threats must be properly divided and studied accordingly. There are three main optimization approaches in MCC, which are focusing on the limitations of mobile devices, quality of communication, and division of applications services. By upgrading the bandwidth limit in wireless network and proper task division mechanism in cloud , we can optimize the task and upgrade data quality. It is to be

noted that designing the future framework solutions should be cost effective and provides better security and performance.

7. REFRENCES

[1] Peter Mell , Tim Grance , "The NIST definition of Cloud Computing", v15
[2] S. Subashini and V. Kavitha ,"A Survey on Security Issues in Service Delivery model of Cloud Computing," Journal of Network and Computer Applications , vol 34, no. 1, pp. 1-11,2011.
[3]Prof. Han Q. and Prof. Abdullah Gani from University of Malaya Research on Mobile Cloud Computing: Review, Trend and Perspectives published in 2012 IEEE
[4]Debasish Jana,Senior Member, IEEE,TEOCO Software Pvt Ltd and BIT Mesra Kolkata Centre Kolkata, India,djana@alumni.uwaterloo.ca and Debasis Bandyopadhyay , Member, IEEE ,Information Security Management System, RS Software (India) Ltd, Kolkata, India debasis.bandyopadhyay@gmail.com : Efficient Management of Security and Privacy Issues in Mobile Cloud Environment published in 2013 Annual IEEE India Conference (INDICON)
[5]Zohreh Sanaei, *Member, IEEE,* Saeid Abolfazli, *Member, IEEE,* Abdullah Gani, *Senior Member, IEEE* and Rajkumar Buyya, *Senior Member, IEEE :* Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges published in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014
[6]D. Popa , Technical University of Cluj-Napoca,Communication Department,Cluj-Napoca Romania ,Daniela.poa@com.utcluj.ro and , K. Boudaoud University of Nice Sophia Antipolis , M. Cremene , M. Borda : Overview on Mobile Cloud Computing Security issues published in serial Electronics and Telecommunication Tom 58(72) Fascicola 1,2013
[7] Security Issues and Challenges of Mobile Cloud Computing from Abid Shahzad and Mureed Hussain, Faculty of Computing SZABIST,H-8/4 Islamabad Pakistan published in International Journal of Grid and Distributed Computing Vol. 6 N0.6 2013.
[8] A Review on Mobile Cloud Computing : Issues , Challenges and solutions, published by Mandeep Kaur Saggi Dept. of CSE , D.A.V. University Jalandhar India , Amandeep Singh Bhatia Dept. of CSE , M.A.U. University India in International Journal of Advanced Research in Computer and Communication Engineering Vol 4, Issue 6, June 2015.
[8] Overview on Mobile Cloud Computing Security Issues published by D. Popa , M.Cremene M. Borda from Technical University of Cluj-Napoca, Communication Department , Str. Dorobantilor. 71-73 CP 400609 Cluj-Napoca Romania and K. Boudaoud from University of Nice Sophia Antipolis in Transactions on Electronics and Communication Tom 58(72) Fascicola 1.2013.
[9] Efficient Management of Security and Privacy Issues in Mobile Cloud Environment published by Debasish Jana
Senior Member, IEEE TEOCO Software Pvt Ltd and BIT Mesra Kolkata Centre Kolkata, India and Debasis Bandyopadhyay Member, IEEE Information Security Management System, RS Software (India) Ltd, Kolkata, India in 2013 Annual IEEE India Conference (INDICON)
[10] Monjur Ahmed and Alan T. Litchfield from Auckland University of Technology, Auckland, New Zealand on paper Taxonomy for Identification of Security Issues in Cloud Computing Environments in JOURNAL OF COMPUTER INFORMATION SYSTEMS 2018, VOL. 58, NO. 1, 79–88
[11] Amin Subandi, Rini Meiyanti, Cut Lika Mestika Sandy, Rahmat Widia Sembiring from *Universitas Sumatera Utara", Medan, 20155, Indonesia* on paper Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification in *Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 1-5 (2017)* ISSN: 2415-6698
[12] Robbi Rahim, Ali Ikhwan Faculty of Computer Science, Universitas Pembangunan Panca Budi, Jl. Jend. GatotSubroto Km. 4,5SeiSikambing, 20122, Medan, Sumatera Utara, Indonesia on paper Study of Three Pass Protocol on Data Security in International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
[13] KashifMunir and Lawan A. Mohammed from University of Hafr Al Batin, KSA
on research paper SECURE THIRD PARTY AUDITOR (TPA) FOR ENSURING DATA INTEGRITY IN FOG COMPUTING in International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.6, November 2018
[14] Mr. Dalila Slimania, Fatiha Merazkaa from LISIC Lab, Telecommunications Department, USTHB University, Algeria on research paper Encryption of speech signal with multiple secret keys in International Conference on Natural Language and Speech Processing, ICNLSP 2015
[15] Hassan Reza, Madhuri Sonawane from School of Aerospace Sciences, Department of Computer Science, University of North Dakota,Grand Forks, ND, USA on research paper Enhancing Mobile Cloud Computing Security Using Steganography in Journal of Information Security, 2016, 7, 245-259

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020
Published Online July 2016 in SciRes.
http://www.scirp.org/journal/jis