Authentication Theory for Mobile Cloud Computing

Vikram Patalbansi
Department of Computer Science
Pacific University ,Udaipur, India

Dr. G. Prasanna Laxmi
Department of Computer Sciences Engineering
Andhra University, India

Abstract- Mobile Cloud Computing (MCC) is a hybrid technology of mobile computing; cloud computing, and wireless cellular technology. With the help of mobile devices like smartphone, laptop, iPod, etc., we can access and process remote data which are stored over the cloud server in real-time through wireless networks. Hence it is lots of chances that sensitive information is susceptible to various types of attacks and anyone can misuse our information. So to establish secure transmission of data among various communicating entities of mobile cloud computing, there must be a good quality authentication scheme that should be implemented. Here in the thesis paper, we review the various authentication scheme proposed by various researchers. After studying various protocols we propose our multi factors anonymous authentication scheme under mobile cloud computing network architecture. In the proposed thesis paper, we used the Fuzzy Extractor function is biometric-based key production technology. To manipulate various multiple authentication parameters like userId, password, IMSI, IMEI, virtual smart card, and UICC, authentication application (Mobile App software) is used over mobile devices and established the session with the cloud server. So our scheme avoids any information disclosure even fingerprint impression also and protects mobile client privacy and improves the security of every entity of Mobile Cloud Computing.

Keywords – Mobile Cloud Computing, authentication, wireless security.

I. INTRODUCTION

The combination of cloud infrastructure and mobile technology or cellular network developed a new computational paradigm model called Mobile Cloud Computing (MCC). In MCC network architecture, resource-constrained electronic mobile devices can utilize computational or storage space resources of cloud server or data center via wireless communication network any time or anywhere else locations. [8] Generally any electronics mobile devices become a major part of our life due to its sharing of information in a flexible manner over mobile wireless network. [7] In the Mobile Cloud Computing (MCC) environment, mobile devices access the resource from the cloud server. Hence before getting any kind of service from wireless networks and cloud servers, the mobile devices must be registered and authenticated. As we know mobile devices having resource and computational constraints, so it is not suitable to perform complex operations in the mobile device for authentication purposes. [11]In MCC, if mobile user and cloud service provider are, both registered with the mobile wireless network and after that mobile device and cloud server will be authenticating to each other with unique authentication protocol to establish secure communication between mobile devices and cloud servers over secure channels at both ends to avoid any vulnerabilities and to ensure the legitimacy of data access.

The research paper is organized as follows. Section "Related Works" describe the related works of different authors in various research papers. In the “Proposed System" section we developed the multifactor authentication scheme. And "Security Analysis" describes the advantages of our protocol”. Finally, the "Conclusion" section concludes this paper.

II. RELATED WORK

In our proposed scheme, we are going to improve the security of Mobile Cloud Computing by proposing advanced lightweight bio-metric based multi-factors anonymous authentication scheme under mobile cloud computing network architecture. [1] During communication in Mobile Cloud Computing (MCC) network architecture, it is necessary to implements secure and private communication protocol to make all entities involved in communicating authenticated and attacks full proof. All the information is transmitted over wireless medium including all mobile devices as well as server-related information are in the form of wireless signals, hence it is so hard to ensure that any unauthorized entities or hackers can get access to transmitted or communicates with any devices involved in MCC network architecture and can steal the private or secret information. So it is a challenge to

authenticated communication of MCC. So authentication and key agreement protocol are necessary for any various communicating electronic mobile devices to ensure the security of information by providing agreed session keys.

As we know the SIM card or IMSI closed circuit, by default, exists into the mobile phone and with the help of IMSI, we can authenticate mobile phones easily because all over the world IMSI number is unique. But in vast Mobile Cloud Computing architecture, every mobile device like laptop, iPad, IoT devices do not have an in-built IMSI closed-circuit chip. Therefore we can conclude that the IMSI chip is not appropriate in a compulsory factor for authentication in Mobile Cloud Computing. If a Mobile phone is stolen or damaged then in this case we cannot do authentication or communication with cloud server. And IMSI chip can be cloned easily by advanced technologies.

[2] In the literature paper of authors Munivel E and Kannammal A. describe the theory of Zero-Knowledge Proof. The Zero-Knowledge Protocol methodologies use the proof of verifying the originality of the prover, whether it is mobile devices or server-side entities in Mobile Cloud Computing, without disclosing further knowledge about the prover to be verifier. The features of Zero-knowledge proof can be divided as follows.

(i) Completeness: "If the requested statement is correct, the honest verifier will prove that the requested statement is true to the honest verifier".

(ii) Soundness: "If the requested statement is false, there is no chance to make fake the result to the verifier that the requested statement is true"

(iii) Zero-knowledge: "If the requested statement is right, and the verifier may not know anything about the prover other than that the requested statement is true".

The user authentication in Mobile Cloud Computing refers to the process of validating mobile user identities so that mobile devices user can legitimately access requested cloud-based resources whenever needed over wireless network communication. From the past two decades, several studies have proposed authentication schema tailored for controlling access to cloud-connected machines as well as cloud servers from mobile electronic devices as well as standalone machines also.

[3] In the initial phases of the mobile cloud computing environment, each mobile device has to register with a specific cloud service provider to access any kind of resources like cloud hardware infrastructure or any cloud services such as IaaS, PaaS, SaaS, etc. For doing registration to any cloud server some of the pre-requisite processes have to be done, we will see later in this paper in detail. After doing the authentication process between mobile devices and cloud servers, the data transmission started over mobile cloud computing wireless network infrastructure. But communication over wireless medium most vulnerable to attack or hacking of information. So a strong authentication scheme must be implemented for secure communication. After mutual authentication between the cloud server and mobile devices in a uniform way by using a single authentication scheme, then the mobile user can access cloud servers from a different location using different networks and different types of mobile devices.

[4] In the literature paper of authors Mojtaba Alizadeh et.al. suggested some theory on authentication in MCC, which can be beneficial in communications and networking service providers by providing a comprehensive insight into the specific domain of various mobile computing services. So that future wireless communication technologies and it's architecture can efficiently and effectively furnish cloud-based resources to mobile users with high security and low footprint. In future research directions in mobile cloud computing towards proposing a suitable authentication scheme that mitigates security issues. For example new 5th Generation (5G) cellular technology launch in wireless communication markets. And it's whole bandwidth of signals divided into different – different slices. For video services, it requires more bandwidth so higher bandwidth slice is allotted to video service and for just calling with audio signals then less bandwidth slice are allotted to audio service. In our next research paper, we will propose a theory on authentication and encryption techniques in 5G Mobile Cloud Computing based upon different slices.

Currently, we will focus on our proposed theory on the authentication technique in Mobile Cloud Computing. In MCC, the mobile devices are equipped with high technology sensors such as touch screen, gyroscope accelerometer, camera, digital compass, biometric scanner, and microphone, etc. that can be used to capture and analyze different inputs. With the help of such kinds of mobile device capabilities, we can utilize its inputs as biometric attributes such as fingerprint, facial, retina, iris, voice, gait, and keystroke pattern, etc. in mobile user authentication over cloud servers as an authentication factor.

[5] Basically in any authentication system or verification system having only two basic entity i.e. one service provider and other one service or information receiver. Here in the case of Mobile Cloud Computing, we have one mobile user and other cloud servers. These cloud servers store all user data and authenticate the user. All the verification and authentication-related information exist in only one server. If cloud server capture or hack by attackers all the credential information and verified data stored in server will be stolen by the attacker.

To make our authentication system more secure proof and to apply more flexibility in storing credential information, we will go with a multi server authentication system so that all credential and authenticated information stored in a

distributed manner over multiple servers. Hence if any attacker successful in getting access to one server then some parts of information is secure over rest of the server in cloud data centre or server.

[10] The authors' Ping Wang et.al suggested in their research paper that due to recent rapid advanced technology, the attacker can perform side-channel attacks and they can hack sensitive information stored in general commercial smart cards by extraction with power analysis and reverse engineering. Hence it cannot withstand off-line password guessing attacks. So instead of the physical smart card to store sensitive information for authentication, we prefer a virtual smart card in our proposed thesis paper.

III.PROPOSED SYSTEM

We are supposed to propose an advance lightweight bio-metric based on multifactor anonymous authentication scheme under mobile cloud computing network architecture. Nowadays the mobile devices equipped with a trusted execution environment like Android and iOS operating systems(OS), various bio-inputted sensors (fingerprints sensor), and various extensible hardware chip slots so that we can embed extended hardware functionality into mobile devices apart from its basic in-built mobile functionality. Biometric authentication functionality is common to mobile devices hence we can include fingerprints authentication in our system so that it can make a strong authentication scheme. Because of the biometric input keys having some advantages like (a) it cannot be lost. (b) very difficult to copy (c) it is hard to distribute and (d) it cannot be easily guessed.

Here, we assume mainly on four entities, including mobile devices, wireless networks access points, trusted third parties, and cloud servers. The various wireless protocols are used between wireless access points and authentication systems in Mobile Cloud Computing likes Transport Layer Security (TLS) protocol and Secure Sockets Layer (SSL) etc. And each entity works under three-factor authentication architectures and following authentication parameters are used in our authenticating scheme for the mobile users as:

1. User ID and Password.
2. International Mobile Equipment Identity (IMEI) for mobile smartphone and MAC (physical) address in case of Laptop or iPod.
3. International Mobile Subscriber Identity (IMSI) or SIM card for internet connectivity.
4. Authentication application API (Mobile App) installed on mobile devices.
5. Virtual Smart card (Likes Cookies stored in the browser over client-server application during web application access).
6. Fingerprint module.
7. Universal Integrated Closed Circuit (UICC) issued by the cloud service provider only to its customer and its identity is unique worldwide and it is like a hardware chip embedded into mobile extensible hardware slots.
8. Cloud Server.
   a) Application (Web) Server (WS)
   b) Authentication Server (AS)

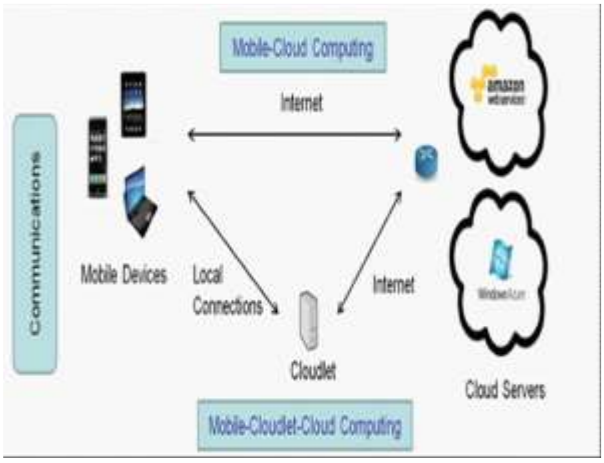

Figure. 1 Three tier MCC architecture

Table 1 : Notation Table

Sr. No.	Symbol	Description
1	Ui	Mobile User
2	WS	Web Server
3	AS	Authentication Server
4	RC	Trusted Third Party Registration Centre
5	user	User Name
6	pw	Password
7	UICC	Universal Integrated Closed Circuit
8	fp	Finger print
9	vsc	Virtual Smart Card
10	B	Biometric information of mobile user
11	Exc(*)	Fuzzy Extractor Generation Procedure
12	Rep(*)	Fuzzy Extractor reproduction procedure
13	$E_Q(m)$	Encryption of message m using key Q
14	$D_Q(m)$	Decryption of message m using Q
15	S_k	Session Key
16	h(.)	Secure One way Hash Function
17	||	Concatenation operation
18	X_{or}	X-OR operation
19	h(user)	Hash Value of user ID
20	h(pw)	Hash Value of user password
21	fp#	Biometric Key
22	fp@	The public reproduction parameter
23	$E_{VIdent}( )$	Encryption function with key VIdent store in virtual smart card
24	$D_{VIdent}( )$	Decryption function with key VIdent store in virtual smart card

In the Mobile Cloud Computing environment , execution of tasks are going through three tier mode like mobile user , 5G wireless cellular network and cloud server. In our propose scheme the trusted third party registration centre exists at 5G mobile network and our privacy aware authentication scheme is developed based on identity based signature scheme including three phases (A) System setup phase (B) Registration phase and (C) Authentication phase.

A. System Setup Phase

1. Mobile Devices: This entity is responsible for generating user ID, password, fingerprint impression, IMEI or MAC code, IMSI code along with Universal Integrated Closed Circuit (UICC) in generating runtime unique identity assigned by cloud service provider. The mobile devices run the client authentication application (Mobile App) with license copy which is installed from the cloud service provider especially designed and configured by the cloud service provider to establish connectivity between mobile devices and cloud service providers' cloud servers. This authenticator application responsible for forwarding credentials information likes user ID, password, fingerprint impression, UICC code, IMEI, IMSI code to the authentication server of cloud server, and trusted third party registration centre(RC). The authenticator application applies the policy to manage access to the virtual smart card credential information. The virtual smart card is nothing but secure storage space that exists into mobile devices memory contains credential information send by the web application server for a unique identity of the mobile device during a particular enforcement session on Mobile cloud computing. The mobile touch screen scanner extracts fingerprint impression of the mobile user and in UICC some unique identity is implemented over closed circuit for accessing authorized service from the cloud server.

2. Trusted Third Party Registration Centre.

Trusted Third-party registration centre (RC) is responsible for verifying requested mobile user and cloud service provider. After verification of both parties, it assigns public keys to both of them.

3. Cloud Service Provider

[9]The Cloud Service Provider manages all the task likes authentication of the mobile user, provides storage to information in a distributed manner, computation of information coming from the mobile devices in the form of web request and assist in communication service to the mobile user. It consists of logical three sub-parts

i) Authentication Server (ii) Application Server and (iii) Cloud Server.

B. Registration Phase

During the execution of this phase, the mobile device user and cloud server are registered with a trusted third-party registration center. Here we are assuming that the 5th Generation Mobile Network operational center is the registration center. This registration center manages the operation of signals concerning various services, managing bandwidth of signal, verification, and establishment of a connection between two or more devices or roaming and billing of devices. To get the services from the wireless mobile network, every entity is verified and registered with a mobile telecommunication switching office operational centre.

i) Registration of mobile devices.

According to Zero-knowledge proof concept, the mobile devices or the user sends it's his user ID and password (pw) by their own choice, IMSI, IMEI or MAC (physical address in case of a laptop, etc.) and fingerprint(fp) to the Registration center (RC) over secure channel connection by encrypting with the hash values of every parameter require for registration. [6]In our proposed system, we are going to use Fuzzy extraction approach reproduction technology to extract a uniformly random string fp# from the bio-metric input value fp means fingerprint impression in a fault-tolerant manner and the random string fp# is treated as input in hash function on behalf of fingerprint impression(fp). This technology consists of two functions as

Exc(*) - Fuzzy Extractor Generation Procedure and Rep(*) - Fuzzy Extractor reproduction procedure. Exc(*) this is a randomized generator function which extracts bio-metric key fp# and public reproduction parameter fp@ from the input biometric information fp i.eExc(fp) = (fp#,fp@). And Rep(*)This is a deterministic function that recovers the biometric key fp# from the input biometric B and the public reproduction parameter fp@.

Step1.The Mobile device calculates the following parameter:

$$DInfo_{MU} = h(user \parallel pw \parallel IMSI \parallel IMEI \parallel fp\#)$$

(in case of smartphone mobile user).

OR

$$DInfo_{MU} = h(user \parallel pw \parallel IMSI \parallel MAC \parallel fp\#)$$

(in case of laptop or iPod mobile user).

Step2. The Mobile user submits all the parameters use in calculating the value of $DInfo_{MU}$ as well as$DInfo_{MU}$valueto a third party registration center (RC).

Step 3. After receiving the registration request, the Registration center (RC) checks the validity of $DInfo_{MU}$ including its all parameter used in the calculation of $DInfo_{MU}$.

Step 4. Then Registration center generated random key r using pseudorandom number generator (PRNG) function and calculate virtual smart card identifier VIdent.

$VIdent = h(r \parallel DInfo_{MU})$.

Step 5. Both the value $DInfo_{MU}$ and VIdent store in the database of the MTSO operational center for further processing. But here the value of $DInfo_{MU}$ is permanently stored in the MTSO database and value of VIdent on temporary basis in the database. VIdent value provides a unique identifier for the encryption of signals for only one session between mobile users and cloud servers.

Step 6. Registration center transfer VIdent value to the mobile device as well as cloud server and in mobile device memory store it like a cookie is used in client-server web application. Every time if a mobile user communicates with the cloud server then this value VIDent appended at the end of the request. This value can be access or manipulated by authentication application (Mobile App) install in mobile devices provided by the cloud service provider.

Hence all the formalities required for registration of mobile users over the registration center (RC) are over.

Algorithm1:Registration:Mobile with Mobile Network
Requirement :
Is_Available (mobile device , mobile network)
hasNetworkAccess(mobile device)
Procedure:
Role_of_MobileDevice
constuser,IMSI,IMEI,fp#
var pw
fp# = Exc(fp) (where Exc() Fuzzy extractor function for finger print module in mobile device)
var $DInfo_{MU}$ = h(user || pw || IMSI || IMEI || fp#)
RC ← $DInfo_{MU}$
Role_of_Trusted_Third_Party_Registration_Centre
recv($DInfo_{MU}$)
var r = PRNG_generate(r)
var VIdent = h(r || $DInfo_{MU}$)
#database ← pointer { store ($DInfo_{MU}$, VIdent)
Mobile ← send (VIdent)
varvsc← pointer{store(VIdent)}

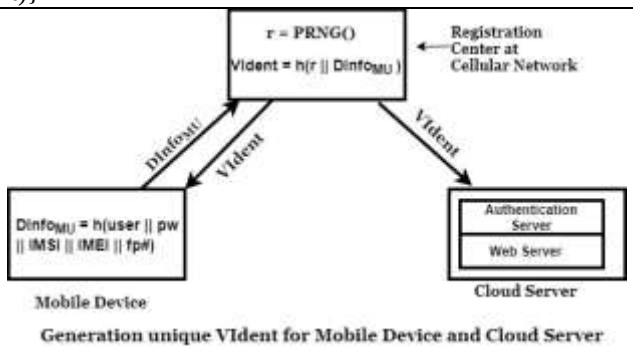

Figure. 2 Generation of Paired Key VIdent

ii) Registration of Cloud Server

Step1. Like mobile user registration, the cloud server also registers with a trusted third-party registration center. But some steps are dissimilar.

Step 2: Cloud Server collects information like MAC address of the machine (MAC), Port number of the application web server (port), IMSI code for wireless internet connection, server user id(Suser), and password (Spw) and calculate following parameter.

cloudServerID = h(Suser || Spw || MAC || port || IMSI).

Step 3: The cloud server transfer this parameter cloudServerID over 5G wireless mobile technology internet connection to a trusted third party registration center (RC).

Step 4 The registration center store cloudServerID values in its operational centre's database for future reference. And registration for cloud server is over RC is completed.

Algorithm 2:Registration: Cloud Server with Mobile Network
Requirement :
Is_Available (cloud_server , mobile network)
hasNetworkAccess(mobile device)
Procedure :
Role_of_Cloud_Server
ConstSuser, Spw, MAC,port,IMSI
var cloudServerID = h(Suser || Spw || MAC || port || IMSI).
RC ← send(cloudServerID)
#database ← pointer{store(cloudServerID)}

C. Authentication Phase

In the authentication phase model, it is divided into three execution sub-parts like mobile user (client), application (web) server, an authentication server.

1. The mobile client: It has two main functions, first it registers to a trusted third party registration center over mobile network operational center. And second, it performs mutual authentication with the cloud server through mobile wireless networks.
2. The cloud server is divided into two logical subparts.
2. a) The application (web) server: It performs the jobs of interacting with authentication application or user agent which was installed on a mobile device provided by the cloud service provider. The main responsibilities of the web server are to get all information from a mobile user and according to a service request by the mobile user; it allocates web components to it. Also, it forwarding the authentication data to an authentication server.

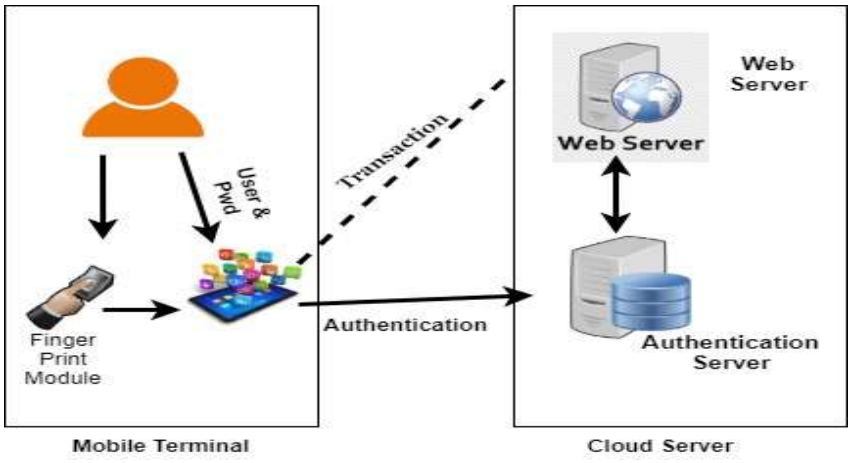

Figure. 3 Role of Authentication Server

2. b) The authentication server: The authentication server performing the main two functionalities. First, it monitors the request of the application server by monitoring the registration information from the mobile client and authorized it to gets service from the application server. Second, it could modify the information for registered clients and then authorized the mobile client and afterward stored all client transaction-related information in the database for future reference.
In the multifactor-based authentication scheme in mobile cloud computing (MCC), we use different authentication features like user id, password, mobile identification number (IMSI, IMEI, or MAC address), various bio-metric information of the user, etc. in combination to pursue good security performance and authentication efficiency.
Here we going to propose enhanced biometric-based multifactor authentication protocol.
As we previously mentioned that cloud service provider (CSP) provides client authentication application or user agent which is installed in mobile devices and registration centre issue a virtual smart card after successful registration process containing all unique identification information stored in the mobile device memory and this information can be access and manipulate by authentication application. This authentication application having all rights to access all mobile device peripherals like virtual smart card data, UICC information and fingerprint module to scan the fingerprint of the user. These authentication applications interact with the authentication server and establish a secure connection between the cloud server and mobile devices.
Step 1: For a more security point of view, in our system, we provide two levels of authentication. One performed by application (web) server by comparing the value of $DInfo_{MU}$ which was stored in TTP Registration Centre (RC) database and calculate $DInfo_{MU}$ which is generated based on same parameter i.e user ID(user), password(pw) unique identification number provided by the mobile network (IMSI or SIM card), mobile equipment(hardware) identification (IMEI or in case of laptop MAC address) and fingerprint random string(fp#) which was calculated by Fizzy Extractor function [Exc(*)].
Step 2. Mobile device client sends the parameter like User Id, password, IMSI, IMEI, and fp# by encrypting every parameter by applying encryption function $E_{VIdent}(*)$ where VIdent is the encrypting key generated by Registration Centre(RC) and stored in mobile device memory virtual smart card and can be accessed by authentication application also.
Step3. This authentication application encrypting every parameter of mobile device identification by using key VIdent which is stored in a virtual smart card.

$$\text{User ID} = E_{VIdent}(\text{user}),$$

$$password = E_{VIdent}(pw),$$
$$IMSI = E_{VIdent}(IMSI),$$
$$IMEI = E_{VIdent}(IMEI),$$

$fp\# = E_{VIdent}(fp)$ and mainly UICC it is a universal identification closed circuit developed by cloud service provider(CSP) for unique identification to any mobile user those wants to gets service from this CSP. It also encrypted like this

$$UICC = E_{VIdent}(UICC).$$

Step 4: All the above-encrypted parameters are sent individually to cloud servers over mobile wireless networks.
Step 5: During all these processes up to authentication of mobile devices, the application server in the cloud server and authentication application (Mobile App) established connection over secure channels.
Step 6: All the encrypted parameters are as $E_{VIdent}(user)$, $E_{VIdent}(pw)$, $E_{VIdent}(IMSI)$, $E_{VIdent}(IMEI)$, $E_{VIdent}(fp)$, $E_{VIdent}(UICC)$ are received by application server.
Step 7: The cloud server registered with the TTP Registration Centre (RC) so that the application server fetch the key VIdent from the RC database which is a temporary database of mobile network MTSO Database.
Step 8: The application server passes all these parameters and decrypting key-value VIdent which is the same as stored mobile virtual smart card to the authentication server.
Step 9: The authentication server apply decrypting function $D_{VIdent}(*)$ to each and every parameter likes

$$user = D_{VIdent}(E_{VIdent}(user)),$$
$$pw = D_{VIdent}(E_{VIdent}(pw))$$
$$IMSI = D_{VIdent}(E_{VIdent}(IMSI)),$$
$$IMEI = D_{VIdent}(E_{VIdent}(IMEI)),$$
$$fp\# = D_{VIdent}(E_{VIdent}(fp\#)),.$$

Step 10 :
Then authentication server apply hash function as follows
$DInfo_{CS}$= h(user || pw || IMSI || IMEI || fp#) (in case of smartphone mobile user).
OR
$DInfo_{CS}$= h(user || pw || IMSI || MAC || fp#)
(in case of laptop or iPod mobile user).
Step 11: Application Server fetches $DInfo_{MU}$ which is stored in the MTSO database and performs a comparison between $DInfo_{MU}$ and $DInfo_{CS}$.
$DInfo_{MU}$?= $DInfo_{CS}$ (Determine whether $DInfo_{MU}$ is equal to $DInfo_{CS}$ or not)
Step 12: If both values are equal to each other than the first level of authentication is successful.
If both values are not equal to each other than the authentication server instructs the application server to send negative acknowledgement messages to mobile client as an authentication failed and break the connections with mobile device client.
Step 13: After first level authentication successful then authentication server decrypting the UICC which is a hardware chip mounted on the mobile device and developed by the cloud service provider and some unique identification mounted on it and this unique identification information also stored in cloud server database at the time of issuing UICC card to the mobile user just like a SIM card in the mobile device.
$UICC = D_{VIdent}(E_{VIdent}(UICC))$.
Step 12 :
If UICC values fetch from authentication server database and UICC value which is calculated by decrypting $E_{VIdent}(UICC)$ is equal then the second level of authentication is successful i.e.
$UICC == D_{VIdent}(E_{VIdent}(UICC))$
Step 13: Then the authentication server sends a confirmation to the application (web) server those mobile users successfully authenticated.
Step 14: Application server sends authentication successful message to mobile device client and according to services demands by mobile users, the application (web) server load respective web components into server processor and send resultant information to the mobile client over mobile wireless networks.
Step 15: Whenever mobile clients send requests to cloud servers for getting some specific service then mobile authentication application append key VIdent at the end of the mobile client request every time. Hence in this manner session is established between the mobile client and cloud server.
Step 16: If a mobile client wants to disconnect the connection from the cloud server or successfully gets all demanded service result then mobile client installed authentication application releases memory occupied by virtual smart card (VIdent key) and instructs to mobile network MTSO database to release or delete VIdent key from it.

Algorithm 3 :Authentication : Cloud Server _authenticate_ Mobile
Requirement:
isAvailable(cloud_server,mobile)
hasNetworkAccess(cloud_server, mobile)
isRegistered(cloud_server,mobile)
Procedure:
var user = h(userId)
var pw = h(pw)
Var IMSI = h(IMSI)
Var IMEI = h(IMEI) or var MAC = h(MAC)
Var #fp = Exc(fp)
Var UICC = h(UICC)
Encryption :
Var VIdent ← store {retrieve(virtual_smart_card)}
Cloud_server ← send (E_{VIdent}(user), E_{VIdent}(pw), E_{VIdent}(IMSI), E_{VIdent}(IMEI), E_{VIdent}(fp), E_{VIdent}(UICC))
Cloud ← send(VIdent) from RC
AS ←send (WS all parameter)
Decryption:
user = DVIdent(E_{VIdent}(user)) pw = DVIdent(E_{VIdent}(pw)) IMSI = DVIdent(E_{VIdent}(IMSI)) IMEI = DVIdent(E_{VIdent}(IMEI)) fp# = DVIdent(E_{VIdent}(fp#)) ,
Authentication Server(AS)
var $DInfo_{CS}$ =h(user || pw || IMSI || IMEI || fp#) (in case of smartphone mobile user). OR var $DInfo_{CS}$ =h(user || pw || IMSI || MAC || fp#)
AS ← send($DInfo_{MU}$) from RC
If $DInfo_{CS}$ == $DInfo_{MU}$
Mobile_authentication_successful
else
Mobile_authentication_fail
AS ← retrieve{ UICC} from AS database
If UICC == DVIdent(E_{VIdent}(UICC))
Mobile_authentication_successful
else
Mobile_authentication_fail
endif
endif

IV.SECURITY ANALYSIS

In proposed authentication algorithm, we use multiple parameters to authenticate mobile devices. First mobile devices must be registered with the registration center (RC) and RC generates the encrypting key and stored in mobile storage. This is stored temporarily and it also is known as a virtual smart card. Here we do not use physical smart cards because it easy to hack and information in it are permanently stored. With the help of this scheme cross channel attacks and brute force, attacks are so difficult. We make use of virtual smart card information as encrypting keys as well as session keys.

By applying encryption over each authentication parameter, we avoid man in the middle attack and eavesdropping attacks. For each session encrypting and decrypting keys are different because RC calculates it by generating a random number and make new operation on authenticating parameters for every new session. Over the cloud server, we distribute the tasks on a web server and authentication server so that cloud machine difficult to hack.

V.CONCLUSION

In proposed thesis paper, we put forward a multi-parameter authentication scheme. Here we authenticate devices with multiple parameters like biometric key and universal identification closed circuit which are unique in terms of all conditions. In our study, we use only two functionality hash function and fuzzy extractor operations. Using fuzzy extractor function we generate a biometric key from fingerprint impression which is easy to calculate. Virtual smart card data treated as encrypting key and session keys. If mobile devices get all services from a cloud server, then the authentication application automatically deallocates memory occupied by the virtual smart card and for a new session, the mobile device has to register again and generate new encrypting key and session key.

REFERENCES

[1] Anonymous and Efficient Message Authentication Scheme for Smart Grid. Libing Wu, Jing Wnag, SheraliZeadally, and Debiao He. Wiley Hindawi, Security of Communication Networks, Volume 2019, Article ID 4836016,https://doi.org/10.1155/2019/4836016.

[2] New Authentication Scheme to secure against the Phishing Attack in Mobile Cloud Computing, Munivel E and Kannammal AWiley Hindawi, Security and Communication Networks Volume 2019, Article ID 5141395, https://doi.org/10.1155/2019/5141395.

[3] MDA: message digest-based authentication for mobile cloud computing, Saurabh Dey, Srinivas Sampalli and Qiang Ye Dey et al. Journal of Cloud Computing: Advances, Systemsand Applications (2016) 5:18,DOI 10.1186/s13677-016-0068-6.

[4] Review Authentication in mobile cloud computing: A survey ,MojtabaAlizadeh, SaeidAbolfazlic, MazdakZamanid, SabariahBaharunb, KouichiSakuraia , Journal of Network and Computer Applications http://dx.doi.org/10.1016/j.jnca.2015.10.005.

[5] Efficient Multifactor Two-Server Authenticated Scheme under Mobile Cloud Computing, Ziyi Han,1 Li Yang,1 ShenWang,2 SenMu,2 and Qiang Liu3, Wiley Hindawi, Wireless Communications and Mobile ComputingVolume 2018, Article ID 9149730, https://doi.org/10.1155/2018/9149730

[6] An Enhanced Lightweight Biometric-based three-factor anonymous authentication protocol for Mobile Cloud Computing.Haixian Chen, Cheng Xu, Zisang Xu, Xiaoham Tu.
IEEE 17th International Conference on Smart City.
DOI : 10.1109/HPCC/SmartCity/DSS.2019.00230.

[7] MDA: message digest-based authentication for mobile cloud computing ,Saurabh Dey1*, Srinivas Sampalli1, and Qiang Ye Dey et al.
Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:18 ,
DOI 10.1186/s13677-016-0068-6.

[8] A Secure Anonymous Authentication Protocol for Roaming Service in Resource-Constrained Mobility Environments, R. Madhusudhan, R. Shashidhara, Arabian Journal for Science and Engineering, https://doi.org/10.1007/s13369-019-04246-2.

[9] Distributed Authentication in the Cloud Computing Environment, Yanzhu Liu, Zhi Li, and YuxiaSun,@Spring International Publishing Switzerland 2015.
DOI : 10.1007/978-3-319-27161-3_74.

[10] Revisiting Anonymous Two-Factor Authentication Scheme for IoT-Enabled Devices in Cloud Computing Environment. Ping Wang, Bin Li, Hongjin Shi, Yau Sheng Shen, Ding Wang, Wiley Hindawi, Security and Communication Networks Volume 2019.
Article ID 2516963, https://doi.org/10.1155/2019/2516963.

[11] Cryptanalysis and Security Improvement of Two Authentication Scheme for Healthcare System using Wireless Medical Sensor Networks.
Jiaqing Mo1, Zhongwang Hu1, and Yuhua Lin2
Wiley Hindawi, Security, and Communication Networks
Volume 2020 , Article ID 504 7379 https://doi.org/10.1155\2020\5047379.