A Prototype of Secure Access Control Framework for Mobile Based Cloud Computing

[1]Jannatul Fardous and [1]Jahirul Kader

[1]Departmet of Computer Engineering, Institute of Science and Technology, Bangladesh.

Corresponding author email: koliiiucja@gmail.com.

Abstract

Mobile Cloud Computing (Mcc) is the availability of cloud computing services in a mobile environment for mobile users. As people enjoyed the advantages of these types of new technologies and services, their concerns about network access control mechanism. Improper use of the data could be done by the accessing of unauthorized access by outside users. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Regarding this issue this research has been done. For ensuring clients data is placed on the secure mode and we enhance access control policies or restricting any user to exactly what he/she should be able to do and secure data/information from any unauthorized access. This paper analysis of the existing works is carried out on this topic also analyses the attacks and issues that occur during authentication in the Mobile based Cloud Computing environment and proposed a framework to meet all mobile cloud access control requirements. It is expected that, this paper can thoroughly be used for future development of secure access control mechanism in mobile cloud users.

Keywords: Mobile cloud computing, Mobile cloud Access Control, Authentication, Mobile Cloud security, Universal unique identifier (UUID), Access Control Provider (ACP).

1. INTRODUCTION

Increased capability of mobile has come new field called mobile cloud computing (MCC) [1] MCC is defined as the combining the cloud computing services into the mobile ecosystem through Internet. According to Mobile Broad Band Connections are forecasted to continue growing mobile worldwide to 5.3 billion in 2018.The MCC virtualizes system by pooling and sharing resources. So the main menaces are to steal personal data (e.g. credit card numbers, passwords, contact database, calendar, and location) .According to the Bank's latest systemic risk survey [2] has noted risks around staff revealing their Bank roles through social media such as Twitter and Facebook. The recent news items include reports of a 400 percent increase in Android malware. Now is a good time to understand the security threat to the mobile Cloud. Within this context, this paper discusses existing mobile cloud access control mechanism and perspective of this trend. Motivated by this fact, we propose a framework of access control method of security service and a key generation algorithms to mitigate the risk in identity management and blocking unwanted access.

2. PROBLEM STATEMENT

If large number of users storing data one central repository and Cloud Service Provider (Csp)is attacked then all data and sensitive information of the users will be compromised. Previously built system lacks in resolving access control problems since this are a huge amount of work knowledge retrieval from this, this paper will focus on strong and unique key management portion. To design and develop secure access control services for mobile devise, there key problems has been identified:

a. Strong key generation for Encrypting and Decrypting data.

Our focus is achieving efficient cryptosystem.So there is a need encrypting data in some format.

b. User authentication and User verification

In order to ensure the integrity of user authentication trusted domain need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.

c. Secure Data upload and download

This paper focuses on the design a framework of access control security service for mobile devices using Hybrid network anomaly detection protocol (HNADP) [3] and hardware authentication method. So data upload from mobile to cloud and download from cloud to mobile should be marinated securely. We are designing a Framework access control services to achieve above goals and allow efficient, flexible and secure access control over cloud environment.

3. THE OBJECTIVE OF THE RESEARCH

Our goals addressed in this paper are to achieve a secure access control service for mobile users on MCC. So the purpose of the research is stated below:

- To identify the appropriate security access techniques those are being used now in the current world of MCC .To Make cryptosystem more viable, keys are also be encrypted and Password protected. So to make data secure both end is also challenge.
- Guarantee the authorized sharers can access the data, while unauthorized sharers couldn't learn anything about data.

3.1 Research questions

- **Research Question 1:** How can we generate a unique Key by using cryptography in combination of hardware authentication and how cloud Intrusion detection protocol used here effectively in practice?

To address this problem the sub research question are:

- **Sub Question 2:** To address this problem how we can use the combination of cryptography with hardware authentication without compromising the performance?
- **Sub question 3**: Though Machine Authentication Code (MAC) is unique Id why we use Universal unique Identifier (UUID)?
- **Sub Question 4:** In what procedure we should be combine cryptography with Hardware for uploading mobile to cloud or cloud to mobile?

4. REVIEW OF LITERATURE

In the year 2013 the work carried out Nitin Y. Suryavanshi , Dinesh D. Puri , Atul V. Dusanev[4] observe that User sends one UDP packet with Processor Id, Machine Authentication code (MAC ID) & user name in datagram. Make IP Validation by using IP gray space analysis. Take a Turing test through the user ID. If communicated IP and Associated Machine identification code (MIC) in white table to allow the access otherwise create black list & denies access.

Advantage Identifying anomalous host by considering IP Gray Space.
Disadvantage It will not capture huge number of anomalies.

In the year 2014 the work carried out Vasantha Sainath K.Aravind [5] has proposed architecture is an enhanced Third Party Auditor architecture is securing the Third Party Auditing by using "Address authentication" technique.

Advantage It was an effective and flexible to provide secure third party auditing.
Disadvantage No investigate to share data ,did not provide security monitoring.

4.1. Anomaly Detection using IP gray space analysis

We use IP gray space analysis technique, which utilizes the characteristics of the IP gray space to identify potential harmful host's .We first present describes a gray IP address. Identification of anomalous external host using IP gray space and relative uncertainty. In the first step, we set an IP active threshold range that range is called as IP active space. Such a threshold setting is called as association rule generation for supervised learning. If source IP address of communication host is comes from IP Active Space then host is a normal user. In contrast, if communicating host uses gray then that will be anomalous host. To implement this step, we must set up thresholds for IP Active Space (192.168.55.1 to 192.168.55.254) if any host crosses that threshold of IP active space then it will be anomalous host. Here we are calculating relative uncertainty (RU)[3]. Relative Uncertainty is standardized entropy. In this study, assume that 100 incoming flows over a day, 10% of which is gray flow as those with sustained suspicious activities.

5. MAC ADDRESSES FILTERING & UUID IDENTIFICATION

MAC address is unique address assigned to almost all-networking hardware such as Ethernet cards, router etc. MAC addresses are 12-digit hexadecimal numbers. There is a special protocol ARP (Address Resolution Protocol) that is used for got that.Though IP and MAC address also is a unique string of numbers that identifies each computer using the Internet. The MAC address quickly changes every time when our devise connects from a wired network to a wireless network, when we are on or off a VPN connection. So That UUID (Universally Unique Identifier) is the best way to ID a machine which is on a per-app basis. It exists in Windows, Mac and many other platforms. UUID is denoted by 32 characters or 128-bit number in length. UUID contains a reference to the network address of the host that generated the UUID, a timestamp record of the precise time of a transaction, and a randomly generated component). Because the network address identifies a unique devise, and the timestamp is unique for each UUID generated from a particular host, those two components should sufficiently ensure uniqueness. It can be generated from the SDK, which will uniquely identify that user to the application itself but not across applications UUID recognizes an app on your Device, and it will stay there until a user completely deletes the app. If any user removes the app completely from his iOS device and then downloads the app again, the ID will change. We can run the above wmic command to get UUID unique number.All the activities that is done in the computer system is stored in it, these information helps the computer to perform better and very efficiently with its hardware. It stores much of the important runtime configuration.

6. RESEARCH METHODOLOGY AND PROPOSED SOLOUTION

In this research work, we reviewed the previous work in order to acknowledge the current knowledge:

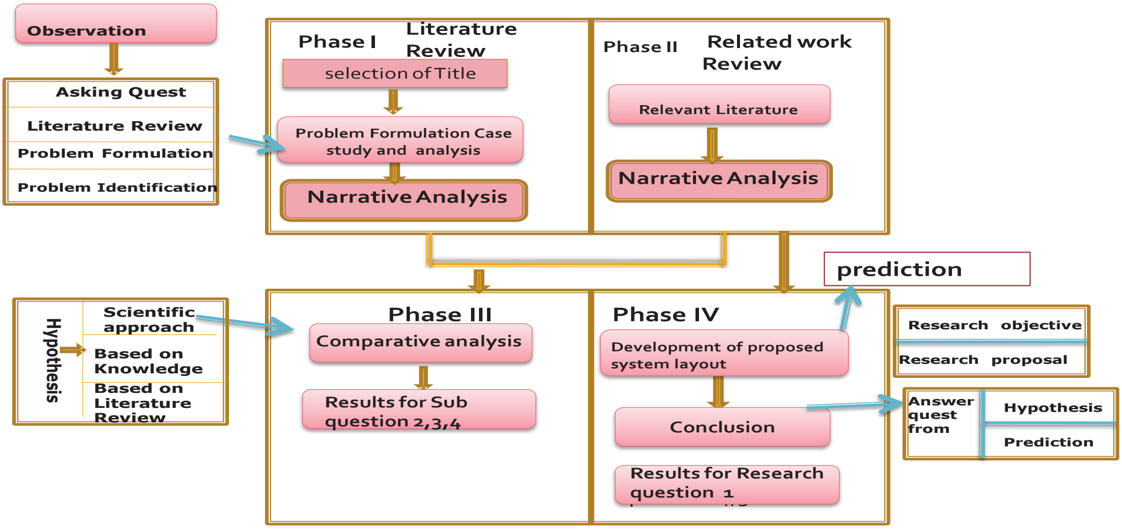

Figure1. Research design

to answer the sub research questions 2,3,4.The goal of this study to answer the research question 1The research design in scientific way is given by the Figure 1 to successfully conduct the paper above steps were taken.

6.1 Assumption consideration

After analyzing various research papers we try to overcome the problem of paper [4][5] .we made assumption that HNADP which issued to detect and prevent the network anomalies but the Drawback is of the paper are

a) There is needed to maintain Database manually

b)Identification of anomaly is based only on Machine Identification Code,

C) There is no provision for how to handle IP spoofing and MAC spoofing.

In our proposed system we have overcame these drawbacks by using hardware authentication and Windows registry itself as a database.

6.2 Identified key factors

To test the assumption, below concepts of key factors were needed to be found out which are:

1. Strong key generation for Encrypting &decrypting data.

2. User authentication and verification
3. Secure Data upload to mobile cloud
4. Data download from mobile cloud

6.2.1 Proposed Solution

To overcome this problem efficient framework for the process is a high demand especially to fulfill of user demand. We had summarized different methods (algorithms technique) and theory which being used to formulate framework and model, derived to provide a better performance, competitive and efficiency to meet the required user need improved lack of previous work.

7. PROPOSED APPROACH

Packets that are sent on the Ethernet always coming from a MAC address, UUID with IP, and Sent to a MAC address with UUID. If a network Adapter is receiving a packet; it is comparing the packet's destination MAC address to the adapters Own MAC address. If the addresses match, the packet is processed, otherwise it is discarded. Protocol to communicate over a network IP addresses is currently 32-bit (ipv4) binary strings which are normally seen by human 223.58.1.10 decimal number. We say these three (unique ID) combination ID MIC i.e. machine identification code by Figure2.

IP	@	MAC	@	UUID

Figure 2. Machine identification code (MIC)

7.1Proposed framework method

The methodology was motivated by the lack of existing work demerits. In order to overcome exiting work demerits, I proposed research scope in listed given below:

1. Secure access control for MCC, ensured by adding unique key with machine identification code (MIC)
2. 2. Avoiding & filtering the unwanted requests coming from the intruder, we proposed monitoring service that is user registry observer (URO) between mobile network and cloud service provider.

3. IP address, MAC-address, UUID addresses are retrieved from Windows Registry of client and compared it with IP and MAC, UUID Addresses which are stored in windows registry of server. In this phase

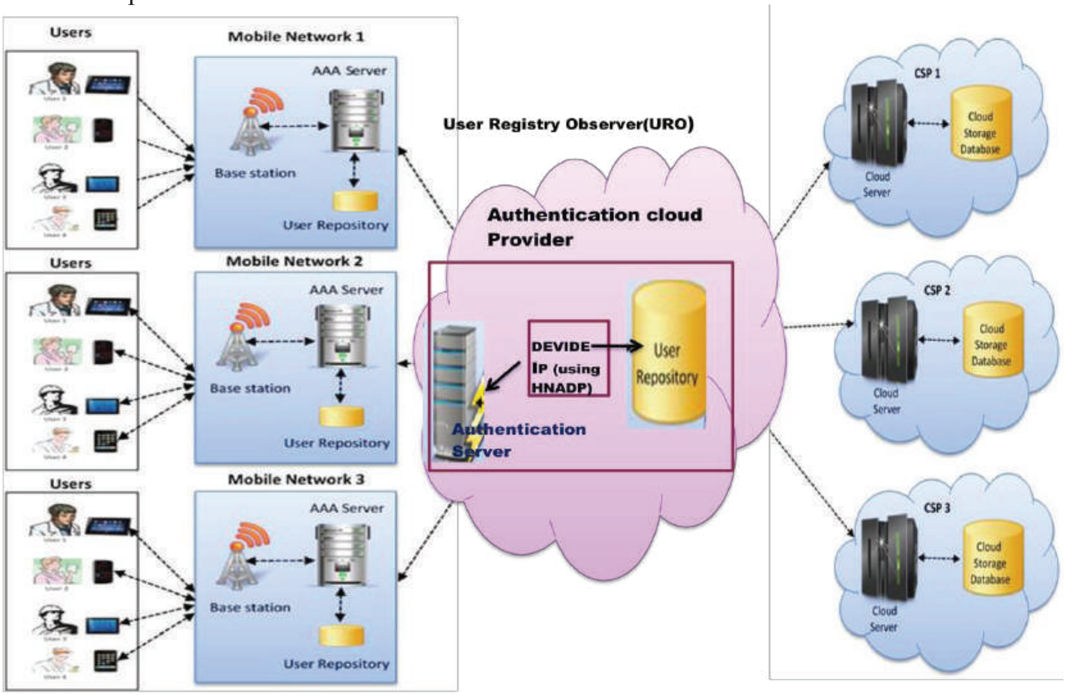

Figure3. Proposed Framework of user registry observer

when any client wants to get services by server then all the identification information is retrieved along with request. If combination of all addresses matches then it is detected as white list client and allowed to access services. Otherwise, denies access.

7.2 Functional units of proposed framework

Figure 4 illustrated on User registry observer which has Authentication server for authenticating the users in mobile cloud environment.The proposed scheme has two important units: User registry observer (URO) and Authentication Cloud Provider (ACPs). The primary mode of communication from the mobile is HTTP over Wi-Fi while the communication between the User registry observer (URO) and the Cloud Service Provider (CSPs) is over HTTPS. The proposed mobile cloud framework has some functional units are:

A .Cloud service provider

It is an entity, which manages Cloud Storage Server (CSS)also manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users.

***B* .Client/owner/Client/**

Owner is a person who owns the data which is to be stored in cloud and utilizes the storage services provided by the cloud service provider.

C. User/data consumer

It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

7.2.1User registry observer (URO)

It is the mediator between the Data Owner and CSP and checks the integrity of the Data stored on mobile cloud. The requested are directed to URO .

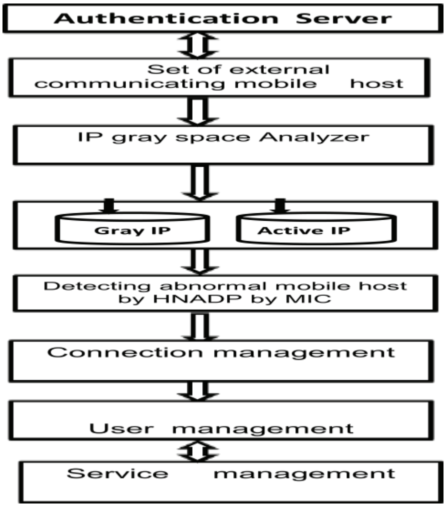

Figure 4.Various part of User Registry observer (URO)

The URO plays major rule in security service for mobile devise which contain authentication server for authenticating not only users but also their rules for accessing their respective services. An owner stores an access control policy in authentication server obtains a URI (uniform Resource identifier) for that policy. We use IP gray analyzer is a network protocol analyzer to detect gray" IP space (namely, collection of IP addresses within our campus network that are not assigned to any "active" host during a certain period of time). We identify and extract potential outside scanners and their associated activities by HNADP gray IP addresses are those within a (campus/enterprise) network that are not assigned to any live host for the entire duration of a given time period, say, a particular day, the collection of which is referred to as the IP gray space of the network. We identifying outside scanners that engage in "sustained" scanning activities. Then using IDS (Intrusion Detection system). The user repository is the place where all user credential data are stored. Communication from the mobile is HTTP over Wi-Fi while the communication between the URO and the CSP is over HTTPS. Authentication Server stores all information which it got from client windows registry[6].

8. APPLIED WORKING PRINCIPLE

Initially the user's requests are communicated over the MN ((mobile network) which holds the Base Station (BS), AAA sever and a user repository .Then User login to the windows application .User selects files he wishes to sync with server. Data should be sending there with MIC. Whenever any data send from the Access control provider(ACP) to the internet a unique key will be generated by proposed algorithm and added with that data from which MAC ID ,it will be identified. So MIC need to add with that data packet which will be sends to data centre of cloud. The time of retrieve data the receiver could identify data by unique key and MAC ID.Then it check normal users using IP gray space analyzer. Here we use windows registry [6] which run on the platform that store registry Client user registration code & also it store this data windows registry server .HKEY_CURRENT_USER which contains the root of the configuration information for the user who is currently logged on. So this stored in formation is associated with the user's profile. So this key is abbreviated as "HKCU. Unique key could be 16 digits with the combination of Alphabet and Numeric. The Alphanumeric key could be so hard to detect by hacker. This key will be hidden except that user only where data would be retrieved. To receive data same process would be applied.

9. ILLUSTRATION COMPONENTS OF URO

There are five components in the URO we already see which are duplicated in Figure 4.All the components are elaborated as follows.

9.1Authentication Server (AS)

All the credentials of the user and the CSPs data are stored in the repository and maintained by the Authentication server. The authentication Server is connected with AAA Server and the CSPs for accessing those credentials. Smart phone 1 connects to cloud server through windows 2008 RADIUS checks using outside communication environment. Then windows 2008 RADIUS verifies mobile device identification and user authorization it creates authentication report also. It sends it access control provider with a session with time stamp.

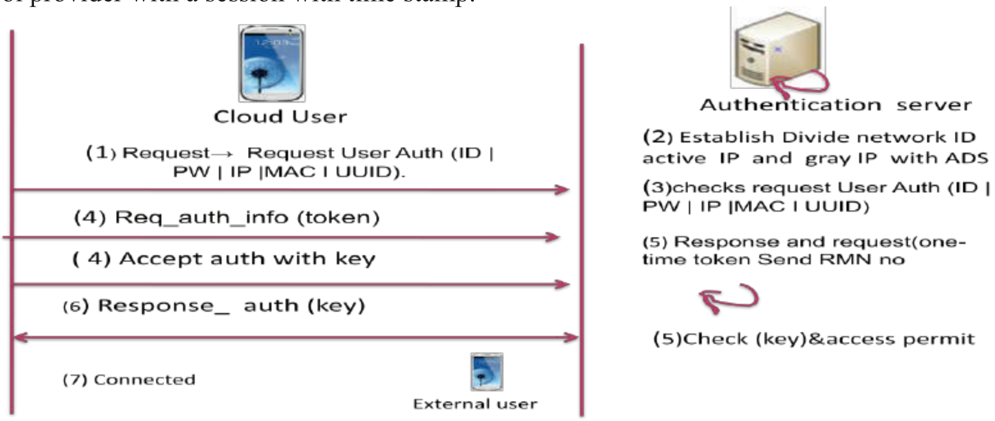
Cloud User
(1) Request→ Request User Auth (ID | PW | IP |MAC I UUID).
(4) Req_auth_info (token)
(4) Accept auth with key
(6) Response_ auth (key)
(7) Connected
External user
Authentication server
(2) Establish Divide network ID active IP and gray IP with ADS
(3)checks request User Auth (ID | PW | IP |MAC I UUID)
(5) Response and request(one-time token Send RMN no
(5)Check (key)&access permit

Figure5. Example of Authentication process

a) IP gray space analyser

We were using here HNAD Server [2] [3]. It detects normal and abnormal users in system. It is used for dividing Gray IP and Active IP is mainly used by machine identification code.

b) Connection Manager Connection Manager is used for managing and monitoring the connections during the authentication.

c) User Manager User Manager manages the user and monitors them during the authentication.

d) Service Manager The service Manager monitors the services accessed by the user. All the authentication activity logs are maintained in the repository of URO

10. STRONG KEY GENERATION FOR ENCRYPTING AND DECRYPTING DATA

Since backbone network (client and server) is developed, then it needs to be secured with a particular algorithm or technique. To achievement of an efficient cryptosystem, we propose key generation algorithm which offers dynamic security on client and server level during communication. When the owner sends a key to the proposed system URO completes the following steps: 1. Registration Phase 2. Authentication Phase 3. Verification Phase

10.1 Registration Phase

The registration process can be done using the mobile devise by the user. During the recognition stage the following are performed by authentication server. The all user machine log profile is already stored in authentication server registry. This phase is the initial phase that is carried out at the both user and URO Side.

11. A PROPOSED PROTOTYPE ACCESS CONTROL FRAMEWORK ALGORITHM

Normal Case
Steps 1: Start
Input a request login from user
Steps 2: Initialize authentication Server
Steps 3: Initialize Gray IP Space analyzer
Steps 4: Check Validity of Machine Authentication Code (MIC)
Steps 5: Check gray IP ValidityIf user MIC, IP, UUID Match, Login Succeed.
Else Request is rejected. Steps 6: stop

Disconnection Case:
Steps 1: Start
Steps 2: if user is disconnected
Steps 2: Check IP gray IP space analyzer
Steps 3: checks data log match in Server windows RADIUS 2008 registry If data cache exists
Performs the access process as explained above
Else
request either forwarded to again devices which holds the replicas. Steps 4: stop

11.1 User Key Generation algorithm

Steps 1: Create initial user registration
Steps 2: Input new devise identification with IP, Mac address &UUID
Steps 3: Add all three IP, MAC ID, UUID Bit no.
Steps 4: Perform converted Total bit no to XOR form.
Steps 5: Shift 1st half at the last half bit no.
Steps 6: Shift 1st 52 bit at the last.
Steps 7: Take 1st 32 bit from total bit no
Steps 8: Convert this 32 bit to 4 digit decimal no
Steps 9: If Valid MIC Identified send SMS this key to User registered mobile no.
Else Display error message

11.2 Example of the key generation:

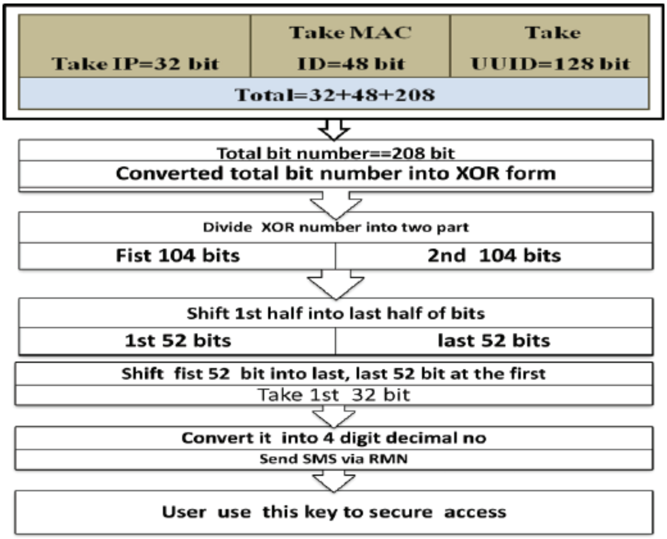
Take IP=32 bit
Take MAC ID=48 bit
Take UUID=128 bit
Total=32+48+208
Total bit number==208 bit
Converted total bit number into XOR form
Divide XOR number into two part
Fist 104 bits
2nd 104 bits
Shift 1st half into last half of bits
1st 52 bits
last 52 bits
Shift fist 52 bit into last, last 52 bit at the first
Take 1st 32 bit
Convert it into 4 digit decimal no
Send SMS via RMN
User use this key to secure access

Figure 6. Example of Key generation process

11.3 Secure upload from mobile to cloud

User should be login to server to manage his file. Then the Authentication server will check. ACP (access control provider) can view report chart. Though the data owner can upload his file to the cloud. If the user have a valid attribute set, then the owner send a key to the user. When the owner send a key to the user then the clock will start counting. After a certain time period, that key becomes an invalid one. So the user should access the requested file within that time limit.

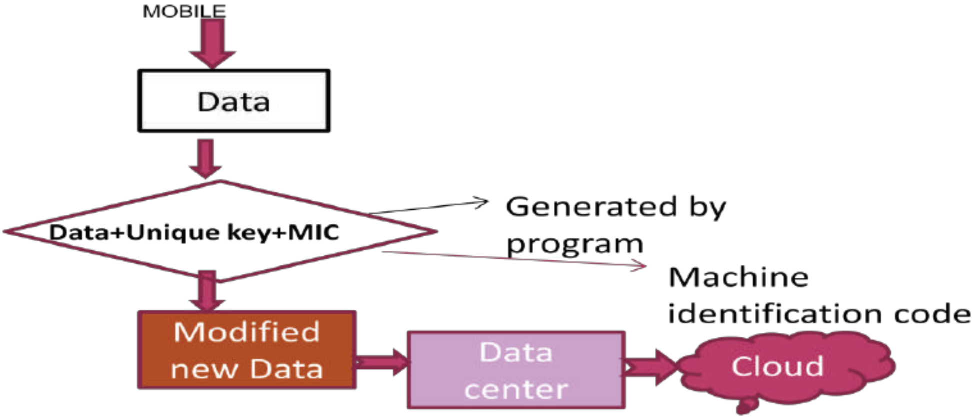

Figure7. Transfer Process by adding unique key and MIC

11.4 Receive process by removing unique key and MIC

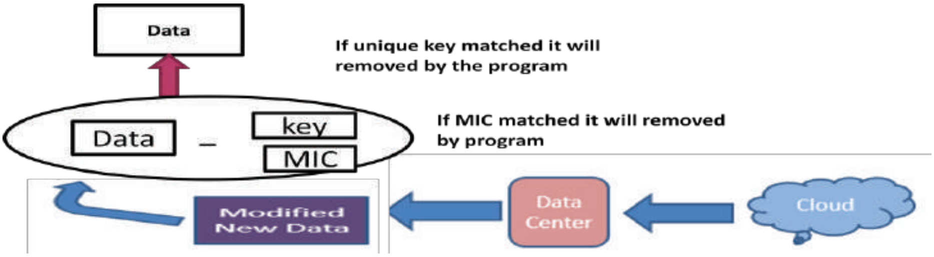
Data
If unique key matched it will removed by the program
Data
–
key
MIC
If MIC matched it will removed by program
Modified New Data
Data Center
Cloud

Figure7. Receive process by removing unique key and MIC

During data receive just reverse process will happen. Before reaching the user data will detached from MIC and unique key by program. This process will happen in ISP Provider or Mobile Operator. If any of key becomes unmatched then data will not be retrieved or received.

12 .AUTHENTICATION SERVER (AS)

All the credentials of the user and the CSPs data are stored in the repository and maintained by the Authentication server. The authentication Server is connected with AAA Server and the CSP for accessing those credentials Windows registry it stored all client profile.

13. VERIFICATION PHASE

The server verified data [7] against their log information stored in database already if it matches the login process accepts otherwise reject it. Then it sends a key which is generated by key generation algorithm has to be send through SMS to user .Then authentication server accepts the user to continue otherwise block user not to proceed further. Also verified in this system that some mobile devices previously log the system or not in order to satisfy prevention phase check Gary or active IP& MIC if matches then proceed. This phase is carried out at the CSP (cloud service provider) Side.

14. CONCLUSION AND FUTURE WORK

Conclusion As far paper review, forums and article I got those issues about discussion. My proposed logic could make another new thought to the world. At the end we would be ensure about access control model of mobile cloud security service for mobile devise by producing those theory.Hence we use here HNDP establishes base line for all users and depends on it decides invalid user. We use windows registry to find out anomaly user. Our proposed framework is A Prototype access control Framework algorithm, Key generation Algorithm ensures uniqueness of key. We would be ensuring about access control model of mobile cloud security service for mobile devise by producing those theory. As of very short time implementation has not been done. In future any of one can implement that to produce high quality security service for mobile cloud environment .So in Future we want to do:

1) It is important to note that the energy consumption [8]forecast of 32 TWh to 43 TWh .We want to concern Battery consumption analysis improvement.

2) We should also want to use here sensor database and Cloud of Things (CoT)

ACKNOWLEDGEMENT

A special gratitude we would like to give Dr Sheak Rashed Haider Noori, Assistant Professor of CSE department, Daffodil International University whose contribution in stimulating suggestions and encouragement helped me to coordinate us especially in writing this report. His constant and energetic supervision, valuable advice have made it possible to complete this paper.

REFERENCES

[1] "Mobile Cloud Computing", International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, vol. -3 , no. -2, 2015.

[2] "Mobile Cloud Computing: Issues, Security, Advantages", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 55, 2014.

[3] "Design of Hybrid Network Anomalies Detection System (H-NADS) Using IP Gray Space Analysis", 2009.

[4] "Anomaly Detection & Prevention by Using Users Fingerprints", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 10, 2013.

[5] "Secured Third Party Auditing in Cloud computing", VIT university Vellore,,India, 2014.

[6] "A Comparative Evaluation of Two Algorithms for Windows Registry Anomaly Detection", Department of Computer Science, Columbia University, New York NY 10027, vol. 10027, 2005.

[7] "A methodology for Development and Verification of Access Control System in Cloud Computing", International Journal Of Advanced Research In Computer Engineering, vol. 4, no. , 3, 2015.

[8] "PDDS improving cloud data storage security using data partitioning Technique", 2013.