ENHANCING CLOUD SECURITY USING MAC ADDRESS

J. Mohamed Aslam[#], Dr.K. Mohan Kumar[*]

[#]Research scholar,[*]Research Supervisor

PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur 613005

(Affiliated to Bharathidasan University, Trichirappalli -620 024)

Corresponding mail: tnjmohankumar@gmail.com

ABSTRACT

Data stored on a cloud server isfaced a number of security problems and threat issues in the user authentication and access control mechanisms. Protecting sensitive business data in the cloud is more valuable because it should be accessed only by the authenticated personnel. The implementation of effective security mechanisms willraise the level of security competence and allows only authenticated individuals by verifying various security parameters given by humans. Sometimes the data is stolen and misused in cloud server in the previous secure authentication methods. Normally, encryption methods are used in the security mechanisms. Another method of implementing security mechanism in the cloud server is by using MAC address. This paper discusses how a MAC address is more beneficial and result-oriented than previous recognition systems.

Keywords: Cloud computing, Authorized user,Security mechanism, Media Access control(MAC); Cloud Service Provider (CSP), Internet Protocol (IP).

DOI Number: 10.48047/NQ.2023.21.3.NQ33015 **NeuroQuantology2023;21(3): 120-140**

INTRODUCTION

The MAC address is the physical address that uniquely identifies each device on a network.This address plays a major role in the communication in between two networked devices using the internet It is also known as Physical address, hardware address, or BIA(Burned in Address).It stands for Media Access Control. Because it is globally unique, no two devices can have the same MAC address. It is based on the data link layer of the OSI model. It is provided by the device's vendor during manufacturing and is embedded in its Network Interface Card (NIC), which is ideally not changeable.The Address resolution protocol (ARP) protocol connects a logical address to a physical or MAC address[01]. A MAC address operates on layer 2 and aids in the identification of devices within the same broadcast network (such as the router) [02].

MAC address format

It is a 12-digit or 6-byte hexadecimal number represented in colon-hexadecimal notation. It is divided into six octets, each of which contains eight bits. The OUI, or Organizationally Unique Identifier, is made up of the first three octets. The IEEE Registration Authority Committee assigns these MAC prefixes to each organization or vendor. Some well-known vendors' OUI examples

eISSN 1303-5150

include:CC: 46:D6 - Cisco 3C:5A:B4 - Google, Inc. 3C:D9:2B - Microsoft 00:9A: CD Hewlett Packard - Huawei Technologies Corporation.The last three octets are NIC specific and are assigned to each NIC card by the manufacturer. Vendors or manufacturers may assign any sequence of digits to the NIC specific digits, but the prefix must match the IEEE specification.[03].

MAC Address's Characteristics

An Ethernet MAC address is a 48-bit binary value that is represented as 12 hexadecimal digits with four bits per hexadecimal digit, but there are a few other MAC address characteristics to be aware of**.**

- MAC addresses have a flat structure; they cannot be routed over the Internet.
- MAC addresses are not used on serial interfaces.
- There is no network or host portion to MAC addresses.
- The frame is delivered to the destination device via MAC addresses.

MAC address types

MAC addresses are classified into three categories:

- MAC Address Unicast
- MAC Address Multicast
- MAC Address Broadcast

MAC Address Unicast:

The Unicast MAC address is used to identify the network's specific NIC.A Unicast MAC address frame is only sent to the interface assigned to a specific NIC and thus to a single destination device. If the LSB (least significant bit) of an address's first octet is set to zero, the frame is intended to reach only one destination NIC.

MAC Address Multicast:

The use of multicast addresses allows the source device to send a data frame to multiple devices or NICs. In a Layer-2 (Ethernet) Multicast address, the LSB (least significant bit) or the first three bytes of an address are set to one and reserved for multicast addresses. The remaining 24 bits are used by the device that wishes to send data in groups. The multicast address is always preceded by the prefix 01-00-5E.

MAC Address Broadcast:

It represents all of the devices in a network. Broadcast MAC addresses are Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF-FF-FF). All of these bits are reserved for broadcast addresses. Frames with the MAC address FF-FF-FF-FF-FF-FF.As a result, if a source device wishes to send data to all devices on a network, it can use the broadcast address as the destination MAC address.

In various situations, cloud computing faces a variety of security issues, including virtualization technology, massive distributed processing technology, service availability, bulk traffic handling, access applications, access data, and authentication. At the moment, the cloud computing platform provides data through an ineffective user authentication mechanism. To access the data and applications, the simple authentication mechanism requires only a password. For easy remembrance, most customers use only weak passwords such as their phone number, name, or related name. As a result, the adversary can easily identify their passwords, access the data and applications, and create security gaps. This is known as a dictionary attack. Smart card-based authentication is another method. It's a two-factor authentication method.The smart card is used to access this customer's credentials, which they are then allowed to use while entering the correct password. Additionally secure

eISSN 1303-5150

the biometric frameworks allow only recognizable evidence of human beings and considering the behavioral or physiological attributes of humans. If sometimes biometric authentication failed or insecure adds another model like using MAC address authentication. In this article the implementation of MAC address for authentication is discussed.

LITERATURE SURVEY

Kamalpreet Kaur and Navpreet Kaur Walia (2014) explained mobile cloud computing is a burgeoning and extensive topic of study. Client and server architecture is transitioning from distributed or cluster to cloud architecture in the age of modern technologies. Data security is particularly important in the Mobile Cloud Environment. As a result, designing the cloud computing security architecture for mobile devices on the internet is one of the primary difficulties also suggested security architecture for mobile cloud computing in this work. [04]

Kyungroul Lee et.al (2016) discussed MAC addresses modification strategies and the resulting security issues. Because the Ethernet MAC address is known to be unchanging, it is highly valued as platform-specific information. As a result, many services are being investigated to use the MAC address. In this study, we provide many strategies for causing a MAC d-of-spo-kino-ng attack. They are not considered to be generic approaches this means that the falsification is difficult to detect, and the outcome is critical in most MAC address-based systems. [05]

Leonardus Irfan Bayu Mahendra et.al (2017) discussed about one of the most crucial components of data transfer to consider is security. Security is primarily concerned with sensitive data, such as government or military information. This study presents a modified AES that modifies the original architecture by utilizing MAC Address. The usage of MAC addresses may improve the unpredictability of AES processes in each machine. [06]

Hitesh Marwaha and Rajeshwar Singh (2019) evaluated cloud computing is the most recent advancement in information technology. It is an internet-based system that requires users to pay based on consumption. However, the most significant barriers to cloud adoption are data privacy and security. The study proposes a mathematical model of data sanitization for giving sensitive data a fake appearance before transferring it to the cloud, as well as a mac address dependent AES algorithm for transferring non-sensitive data and sanitized data. [07]

J. Mohamed Aslam and Dr. K. Mohan Kumar (2022) explained many other forms of assaults, such as data theft, malware, and phishing, are always taking place on cloud storage. This article examines the proportion of different assaults and losses caused by attacks, and discovered that the data breach attack is the most common. [08]

J Mohamed Aslam and Dr. K. Mohan Kumar (2022) discussed before sending data to cloud storage and talked about the encryption technique. This strategy can limit data leaks to some extent. This paper presents a suitable encryption technique on the client side that increases data security in cloud storage. [09]

J Mohamed Aslam and Dr. K. Mohan Kumar (2022) evaluated data hosted on a distant server in cloud computing offers many security concerns and threat issues connected to user authentication and access control systems. The new biometric technology is one-of-a-kind, providing rapid and frictionless authentication. This study demonstrates how a biometric system is more helpful and results-

eISSN 1303-5150

oriented than previous recognition systems that were based on assumptions. [10]

Any operating system can easily find or check the address of a computer device. Every device connected to the home network has its own MAC address, but if our individual system has multiple network adapters, such as an Ethernet or wireless adapter, each adapter or NIC has its own MAC or physical address.

Steps to find the MAC addresses of a device on a windows operating system

Step 01: Press the Windows key or click Window Start.

METHODOLOGY

Figure 01: Windows start Menu

Step 02: Type cmd into the search box to open the command prompt.

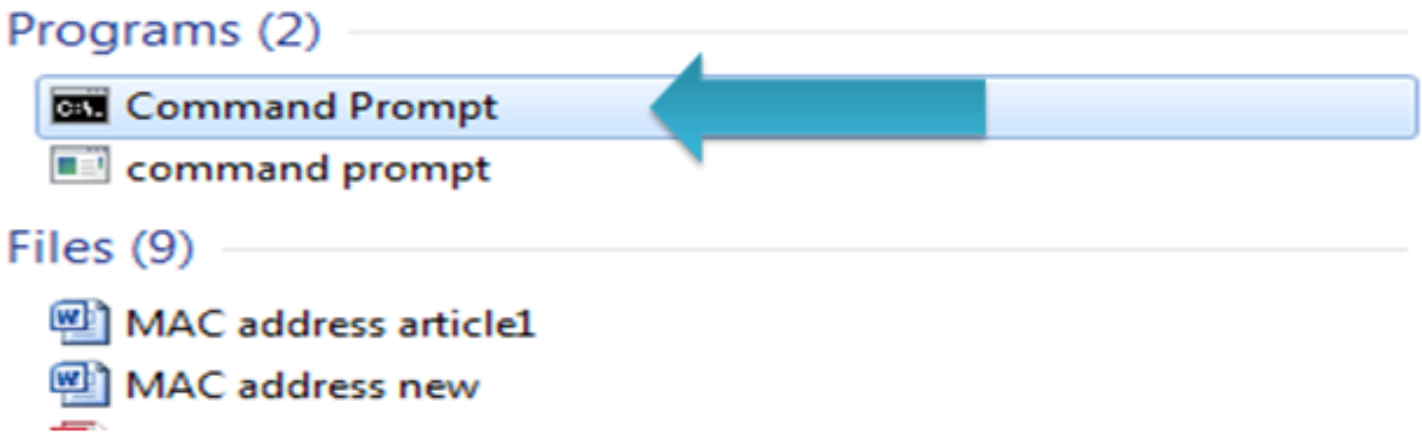

Figure 02: Command Prompt

Step 03: Press the Enter key, the command prompt window will appear, as shown in the image below**.**

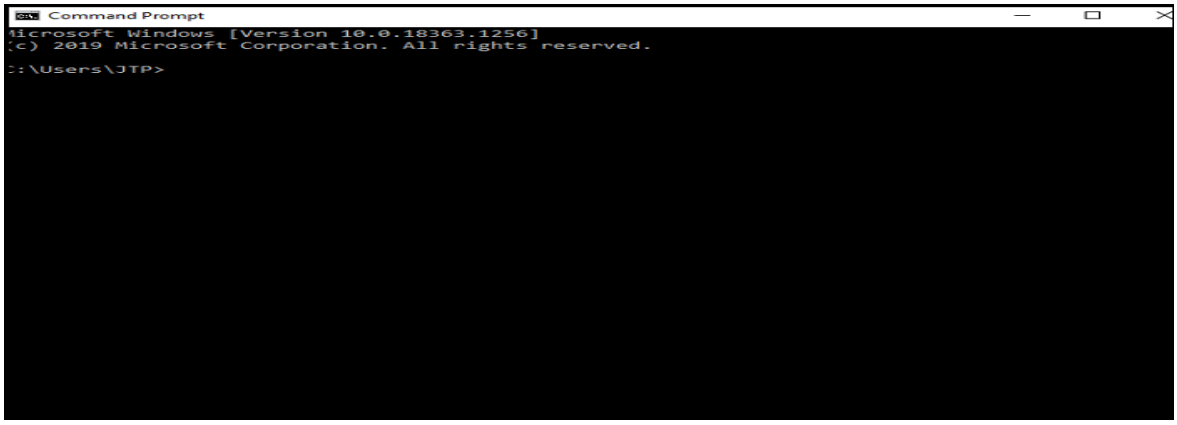

Figure 03: Command Prompt Page

Step 04: Enter the command ipconfig / all and press enter.

Step 05: It will display various information; scroll down to find the physical address. Each physical address corresponds to system device's MAC address.

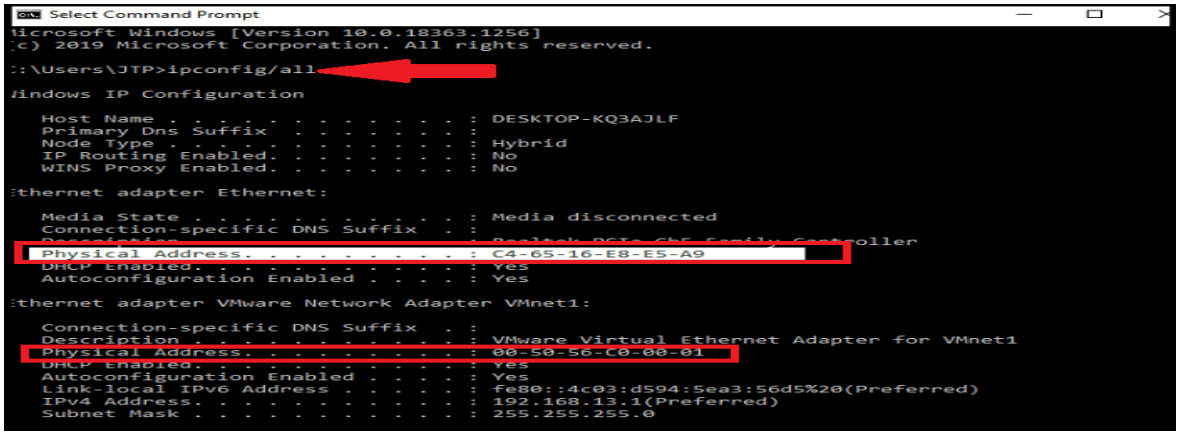

Figure 04: MAC Address (Physical Address)

As seen in the preceding image, there are two physical addresses with different values: one for the Ethernet adapter and one for the VMware network adapter.

This proposed system implementation part contains three sections. They are

i). New user Registration

ii). Assigning MAC addresses to the monitoring system

iii). Login page of existing registered users

eISSN 1303-5150

Phase 1: New User Registration

The following Figure-05 shows the architecture of new user registration**.**

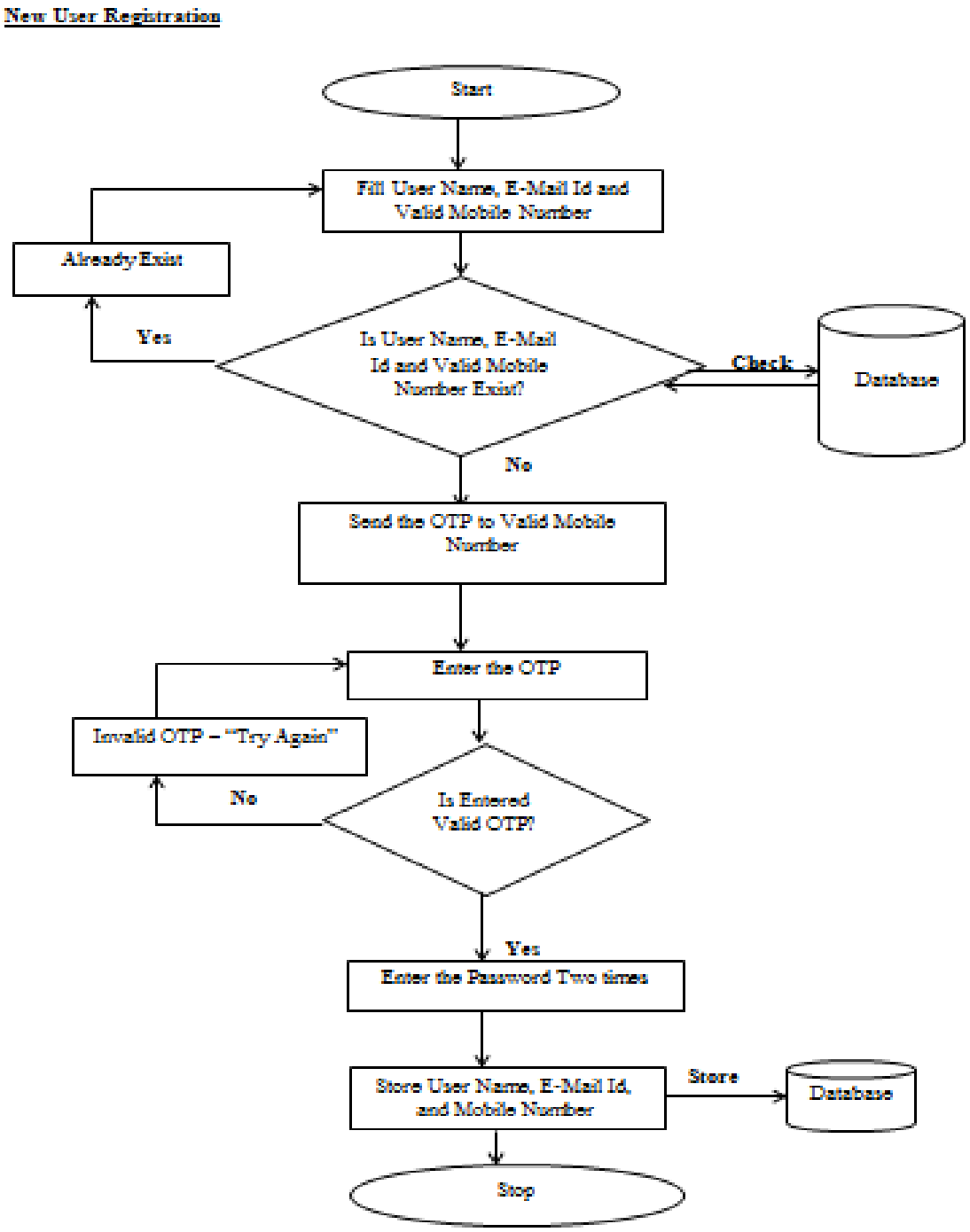

Figure 05:The Flow Diagram of New User Registration

In the First Phase, a new user account must be registered. So, a new user name, e-mail, and mobile number of the user must be given. After providing this information, the information will be checked in the database.Then an OTP message will be sent to the registered mobile of the user and if the user registers correctly user canprecede to the next level otherwise the registration will be rejected. After registering the OTP correctly

enter the new password twice then all the above information of the new user will be properly stored and secured in the database of the cloud.

Phase 2: Assigning MAC addresses to the monitoring system

The following Figure-06 shows the architecture of assigning of MAC address.

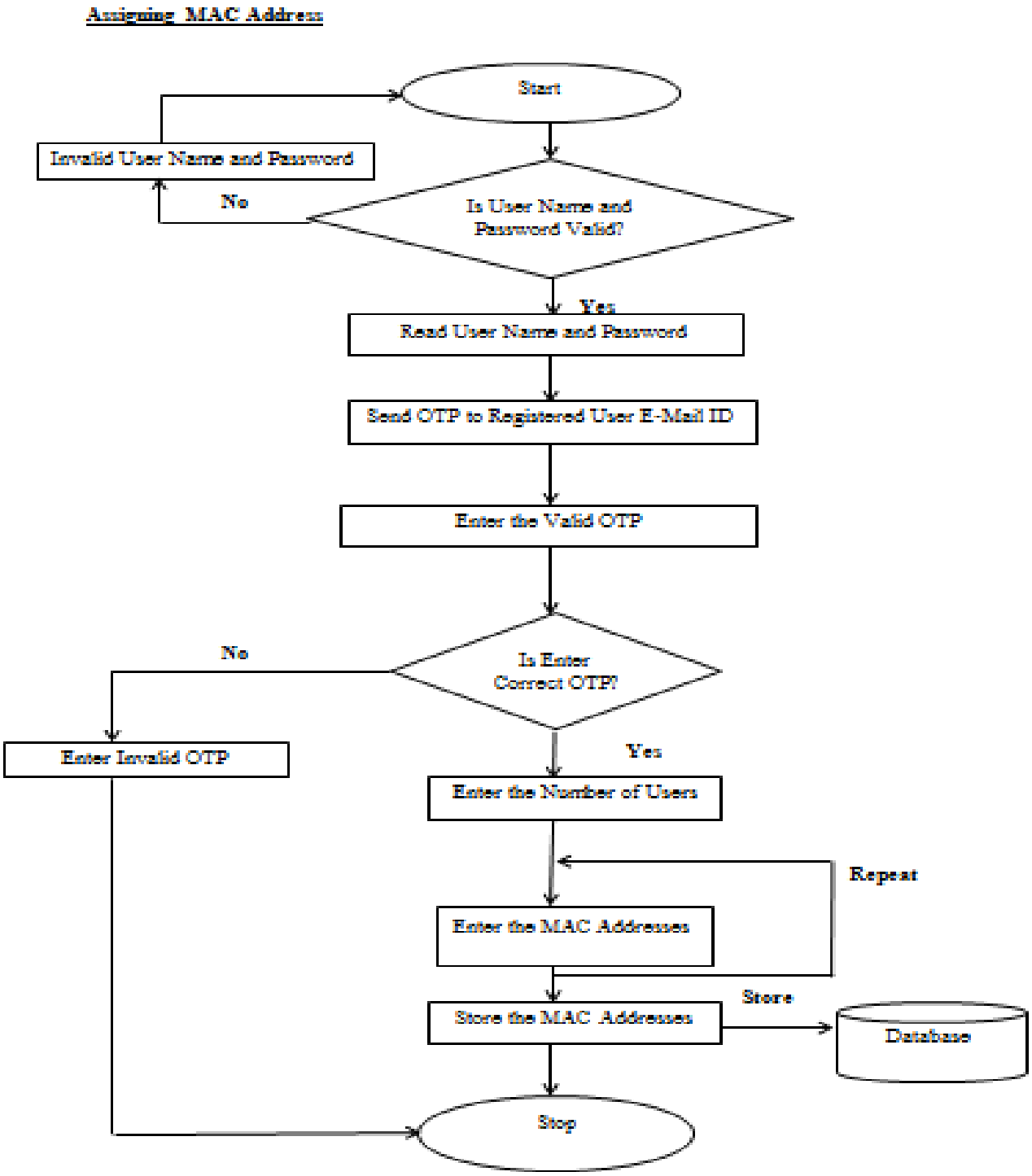

Figure 06: The Flow Diagram of MAC AddressAssigning

The second phase is to register the MAC address, after entering the user name and password, an OTP message will be sent to the user'sregistered E-Mail ID. If the user enters correct OTP, it will go to the next step; otherwise, the request will be rejected.Afterentering the valid OTP, the user needs to confirm how many computers to handle and enter the MAC addresses of each computer. The MAC addresses of all computers in the organization will be stored in the cloud database.

Phase 3: Login page of existing registered users

The following Figure-07 shows the architecture of assigning of MAC address.

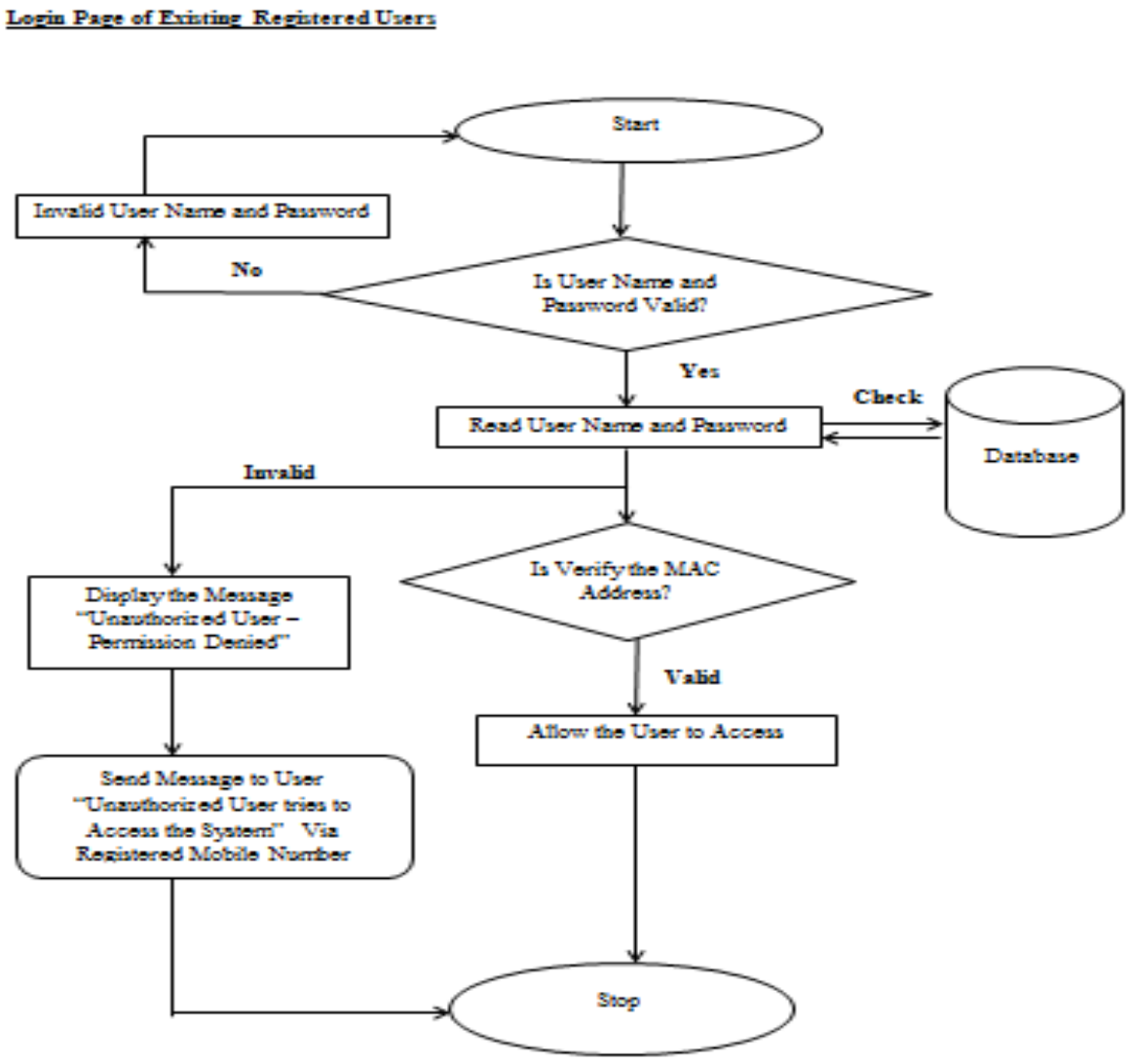

Figure 07: The Flow Diagram of Existing Registered Users

In the third phase, the registered user should enter the user name and password correctly. If the user enters correctly, the system will check the MAC address using the database which stored the user's MAC addresses. If it matches, then the registered user will be allowed to continue.Otherwise, the system will not permit and send the message "Attempt to access by the unauthorized person" to the authenticated user's mobile number automatically. Thus,this proposed system prevents the mishandling of unauthorized person.

RESULT AND DISCUSSION

The following Figure-08shows the view of Sign-up page. In this page the user should fill out with their new user name, email address, and other mandatory information.

Figure 08: New User Sign up Page

The following Figures09 and 10 show when the user name and email address were already in the database

Figure 09: User Namealready Exist Page

eISSN 1303-5150

Figure 10: E-Mail Id already Exist Page

The following Figure-11will be displayed when the user enters the correct OTP received from the mobile number.

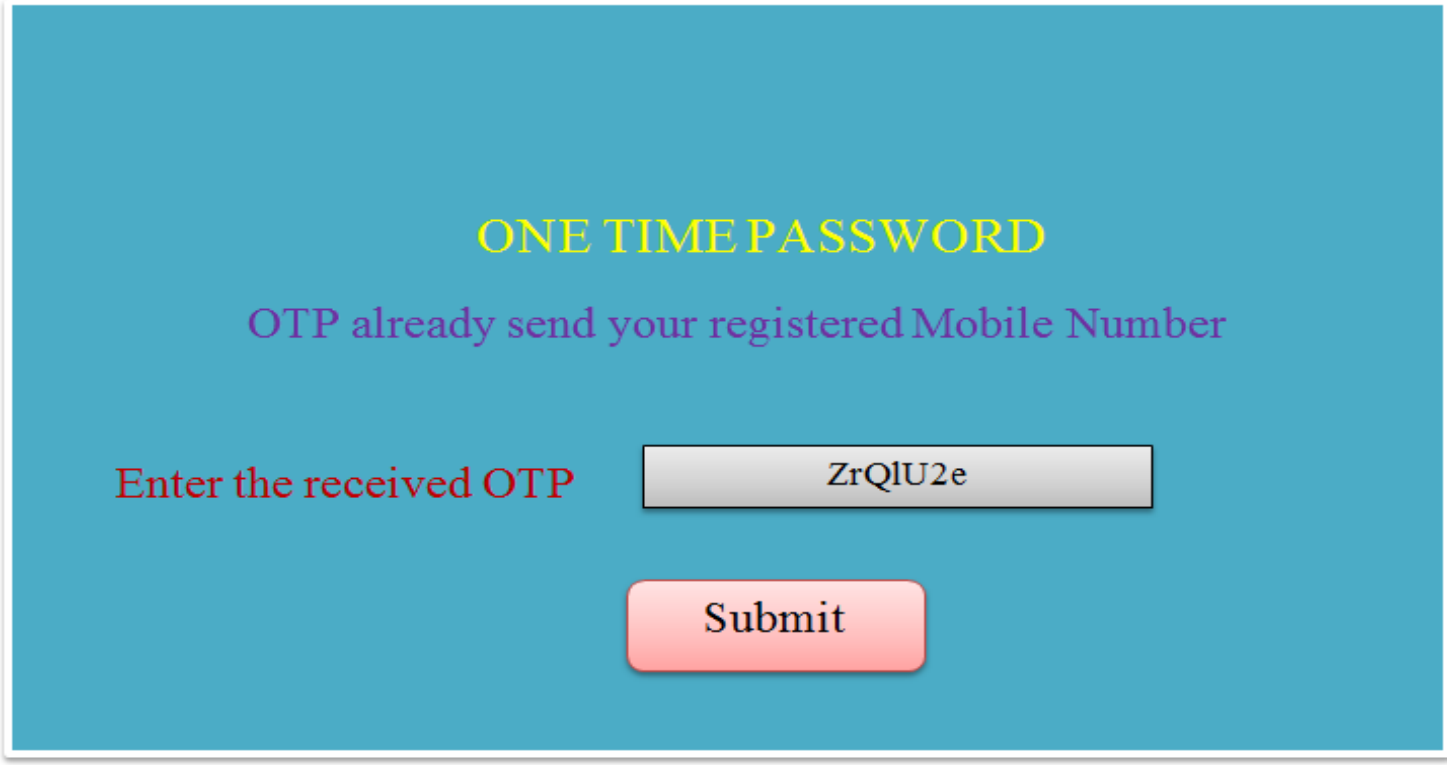

Figure 11: OTPRegistration Page for New User

The following Figure-12 will be displayed when the user creating a new password.

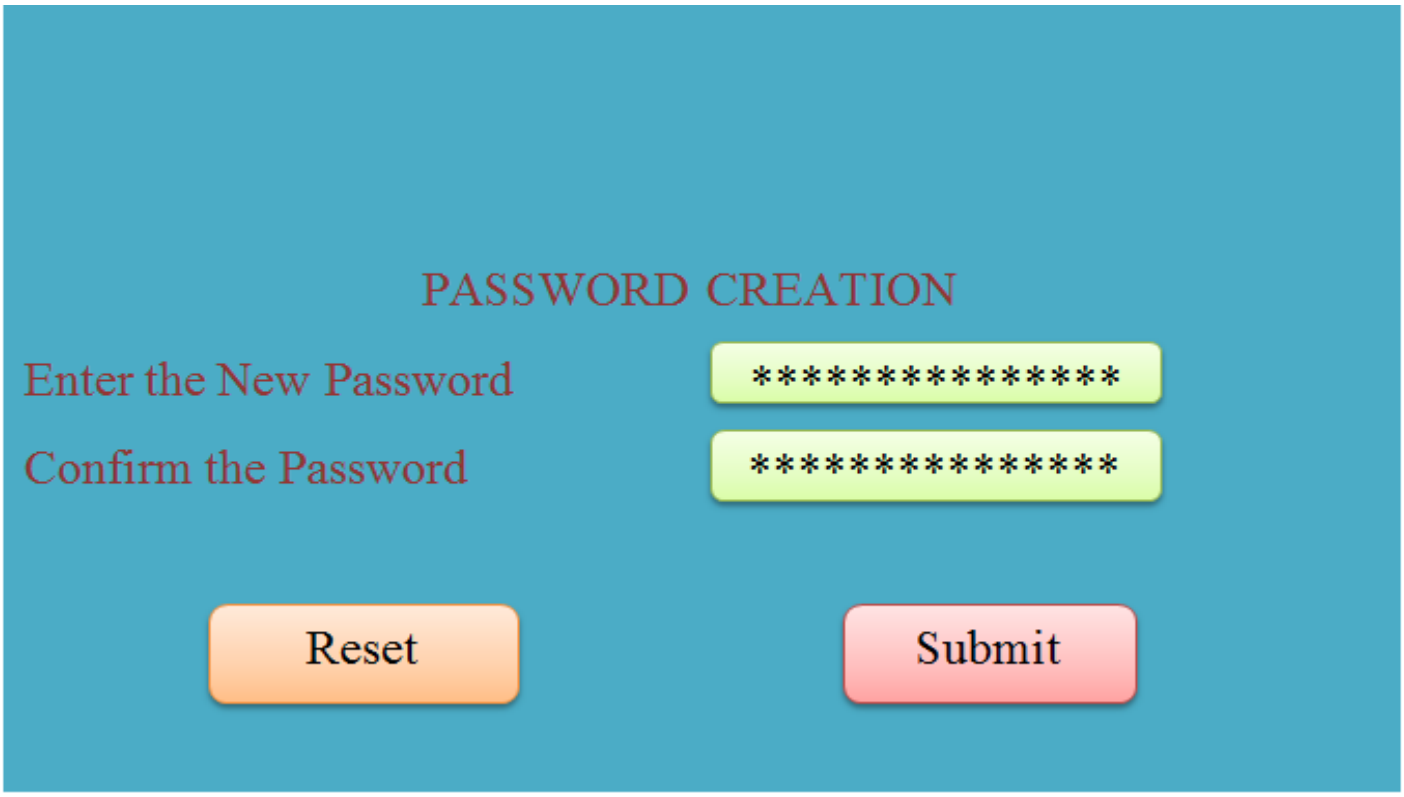

Figure 12:Creation of New Password Page

The following Figure-13 showsif everything is in correct, the following information will appear on the screen.

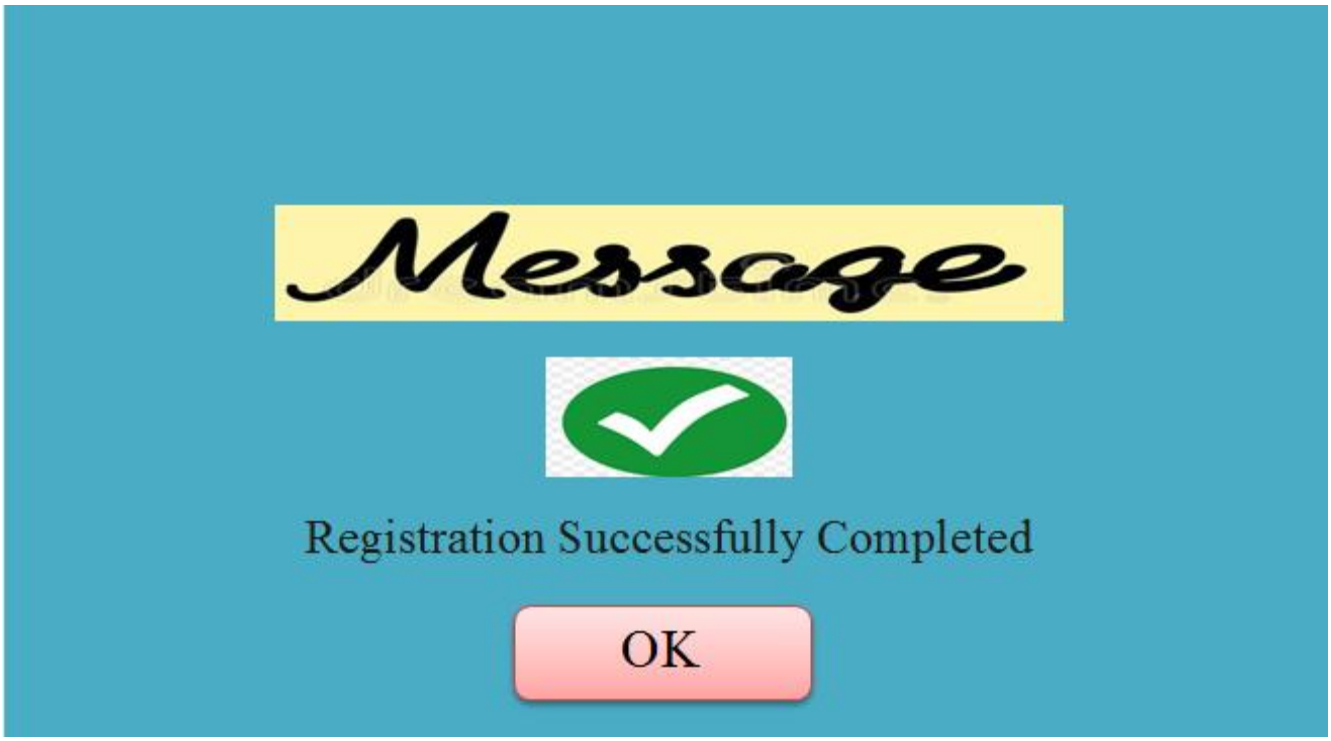

Figure 13: New User Registration Page

The following Figure-14 shows the view of sign in page for assigning the MAC Address.

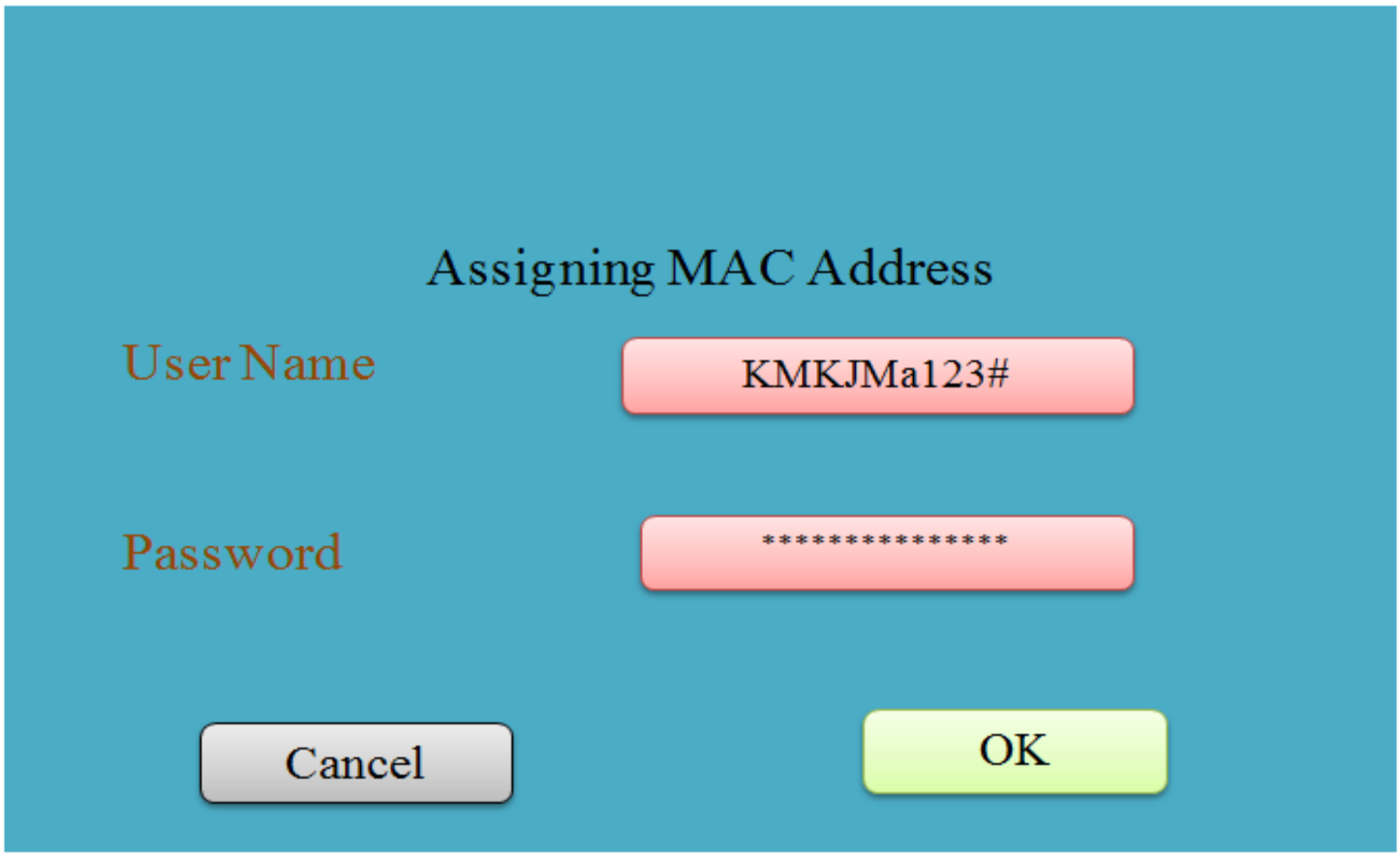

Figure 14: Sign-In Page for MAC Address assigning

The following Figure-15 will be displayed when the user enters the correct OTP received from the E-mail id.

eISSN 1303-5150

Figure 15: OTP Registration Page for MAC Address assigning

The following Figure-16 will be displayed when the user enters the number of user registred the MAC address.

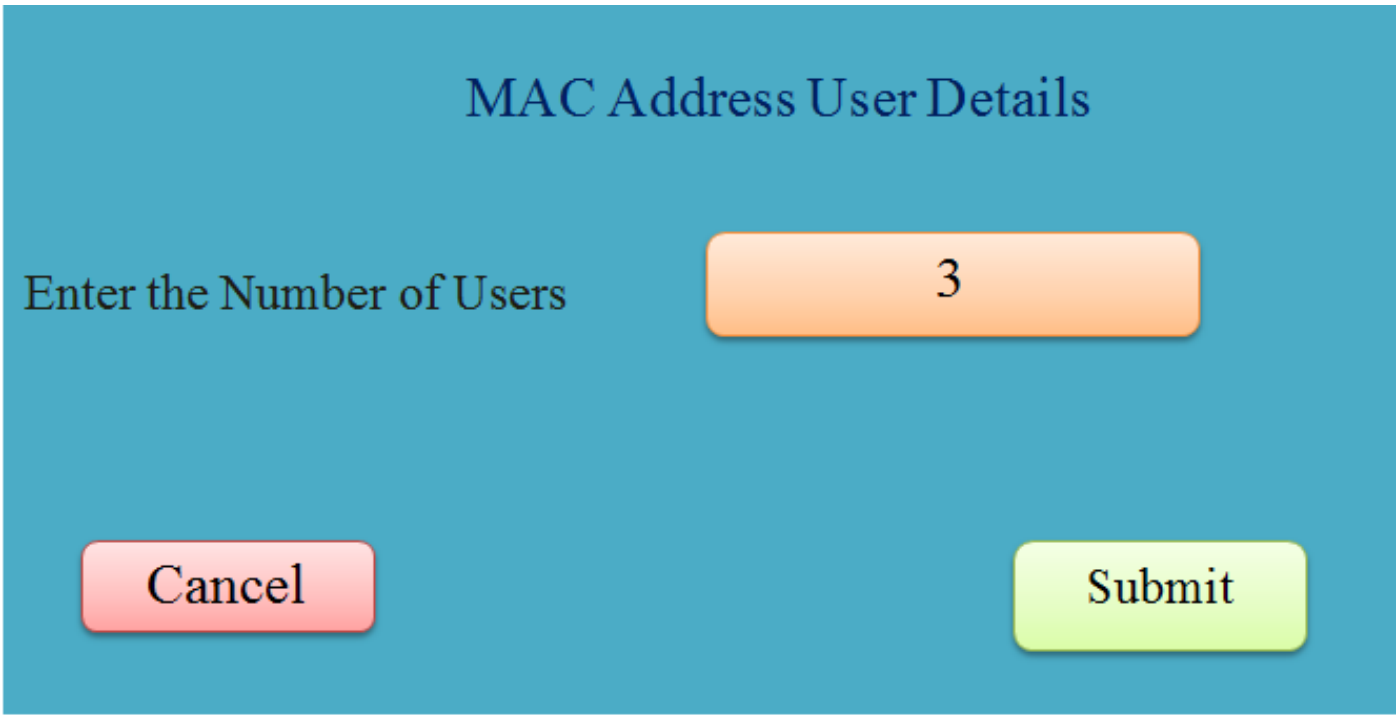

Figure 16: Enter the MAC Address User Details Page

The following Figure-17 will be displayed when the user enters the MAC address details.

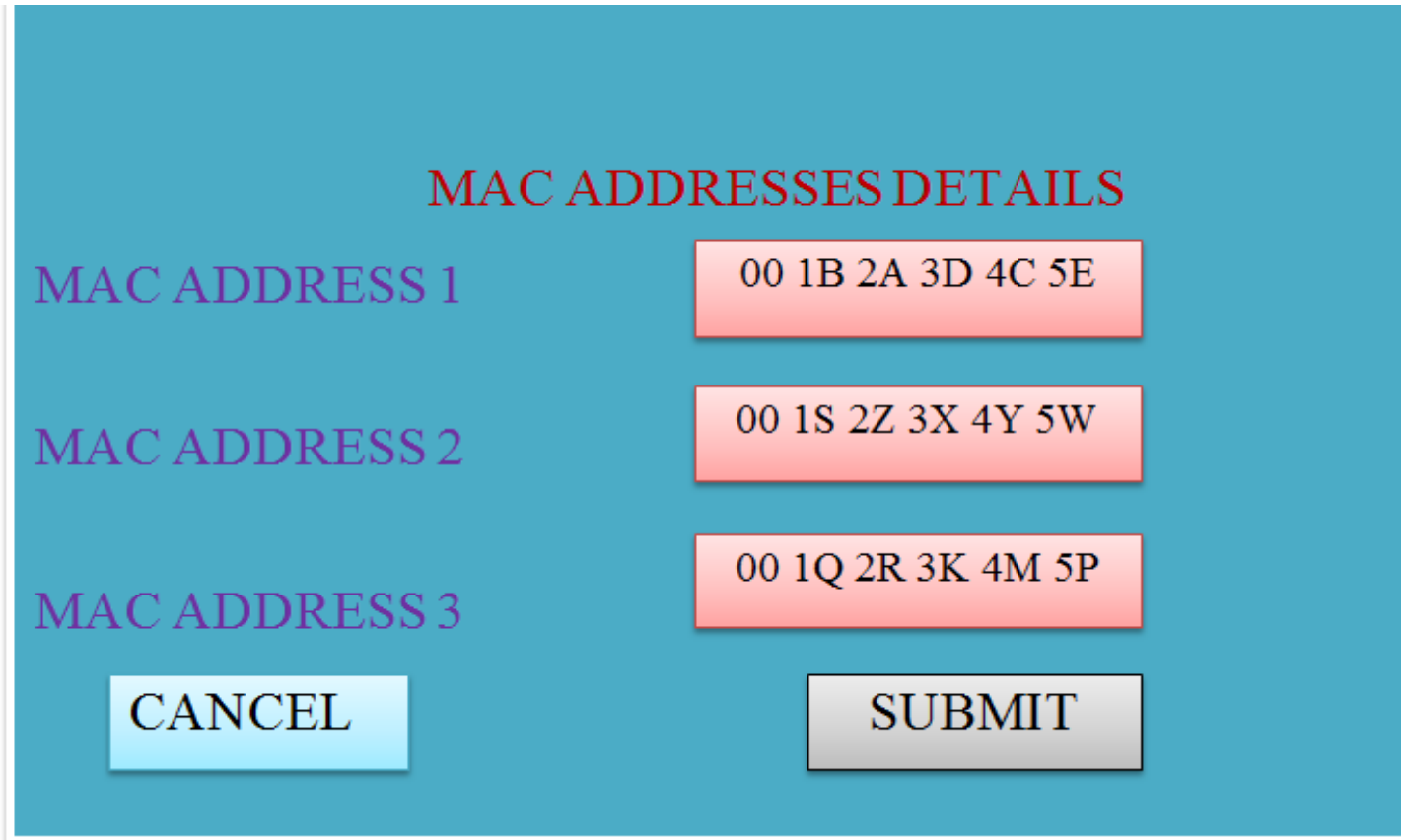

Figure 17: Enter the MAC Address Details Page

After entering MAC addresses, the system will save the addresses and display the messageas in the Figure-18.

Figure 18: TheMAC Addressesstored conformation Page

While accessing the information, the user should fill out the login interface form. The login interface form for the registered user is look like in the Figure-18 below. The user should enter their user name as well as E-Mail id. If they enter this information, the system will send OTP (Figures 19 and 20) to the user's registered email address.

Figure 19: Sign-In Page for Existing User

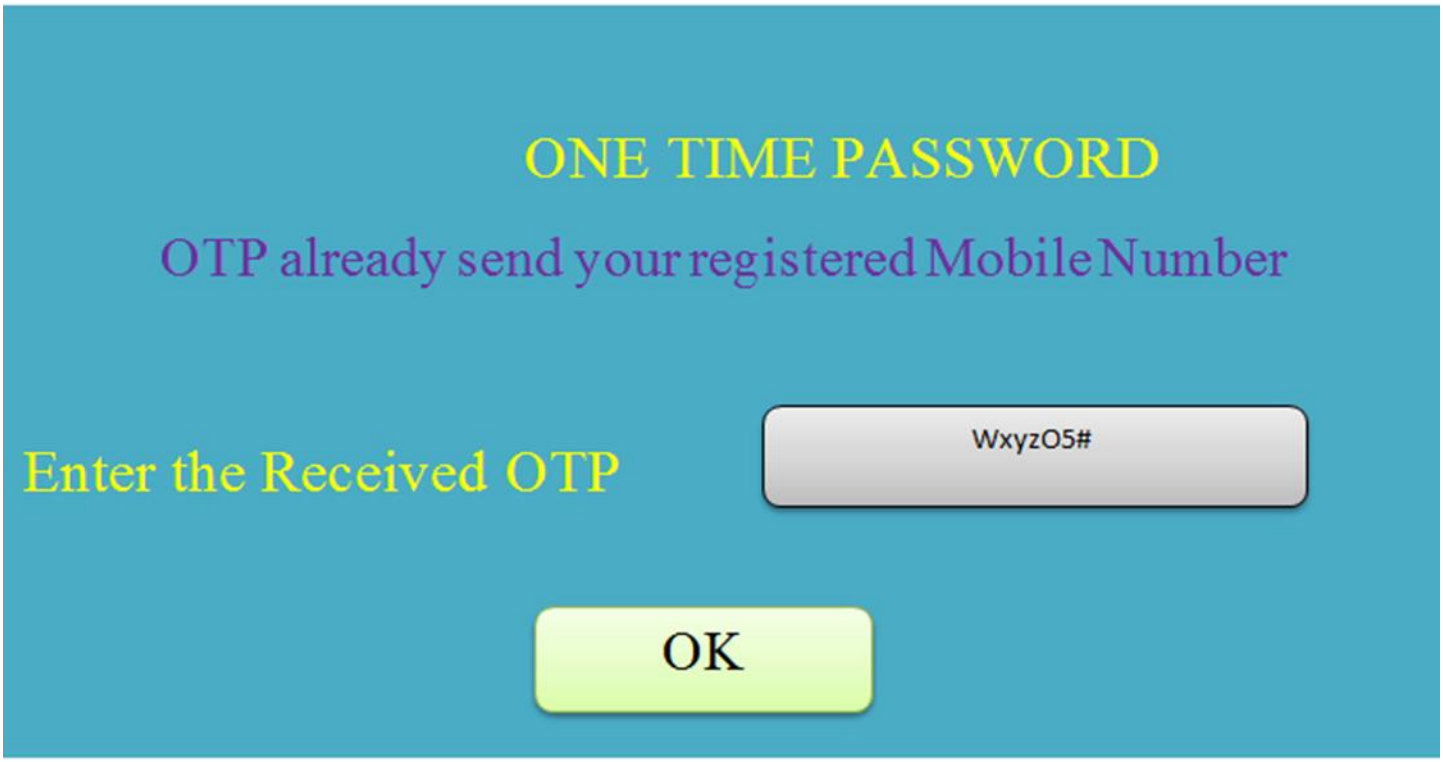

Figure 20:OTP Registration Page for Existing User

If username and password are correct, then the system will compare the MAC address with the database. If any mach found then the following message will be displayed in the Figure below 21.

Figure 21: The Page of Accessing Allowed

Otherwise, the system will display the following message, as shown in Figure-22.

Figure 22: The Page of Access Denied

PERFORMANCE ANALYSIS

The Table-01 below shows the performance analysisof various methodsusing online cloud-sim simulator.

Table 01: Performance Analysis of Various Methods

S.NO	METHODS	TYPES OF RISKS	TOTAL NUMBER OF USER ATTEMPTS	% OF SUCESSS RATE OF USER
01	User Name And Password	Weak Or Commonly Used Passwords	100	52
02	One Time Password (OTP)	Misconfigured Cloud Buckets	100	66
03	Bio-Metric Authentication	Missing Multifactor Authentication	100	73
04	URL Authentication Based	Poor Access Management	100	81
05	MAC Address Authentication	Misconfigured Cloud Security	100	93

The following Figure-23 graphically shows the performance analysis of above Table-01.

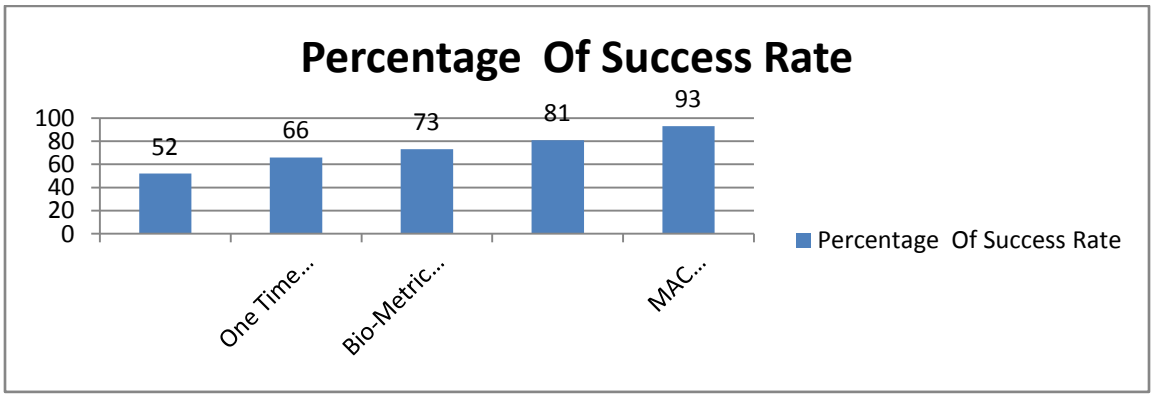

Figure 23: Bar ChartDiagram of Performance Analysis

CONCLUSION

In today's digital world, the data are stored and accessed in the cloud by its users. Every day the usage of cloud is in increasing stage. Protecting the cloud data from the unauthorized person is a challenging task. Because of the prevalence of online fraud, implementing new cloud security techniques is critical. In this work a new kind of protection mechanisms is provided to tighten security flaws. Thus, the proposed system will provide its users with a risk-free cloud computing environment.

REFERENCE

[01]. Mohammad Firoz Alam,Jai Singh and Ravinder Kumar, "Evaluation of Internet Protocol Addressing and Comparison between Ipv4 & Ipv6: A Study", International Journal of Research (IJR), Volume: 02, Issue No: 07, PP: 387-392, 2015.

[02]. Atena Shiranzaei and Rafiqul Zaman Khan,"Internet protocol versions — A review", 2nd International Conference on Computing for Sustainable Global Development (INDIACom), @IEEE, 2015.

[03]. A Arthi Ramani, Salim Vhora and S Sanyal, "The Next Generation Internet Protocol", Informatica 17.

[04]. Kamalpreet Kaur and Navpreet Kaur Walia, "Enhancing The Mobile Cloud Server Security by MAC Address", International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume: 03, Issue No: 06, PP: 2505-2510, 2014.

[05]. Kyungroul Lee, Hyeungjun Yeuk, Kangbin Yim, and Suhyun Kim "Analysis on Manipulation of the MAC Address and Consequent Security Threats ", MIST'16, Vienna, Austria,2016.

[06]. Leonardus Irfan Bayu Mahendra, Yehezkiel Khakham Santoso,and Guruh Fajar Shidik "Enhanced AES using MAC Address for Cloud Services" , International Seminar on Application for Technology of Information and Communication (iSemantic), PP: 066-071,2017.

[07]. Hitesh Marwaha and Rajeshwar Singh, "The Secure Migration of Data to Cloud using Data Sanitization and MAC address based AES", International Journal of Recent Technology and Engineering (IJRTE), Volume:07,Issue No: 06, PP: 1974-1980,2019.

[08]. J.Mohamed Aslam and Dr. K. Mohan Kumar, "Assessment of Security Attacks in the Cloud", International Journal of Mechanical Engineering, ISSN: 0974-5823, Volume: 07, Issue No: 01, PP: 2599-2606, 2022.

[09]. J. Mohamed Aslam and Dr. K. Mohan Kumar, "Assessing the Performance of Encryption Algorithms to Enhance Cloud Security in Client Side", ISSN: 0972-3641, Volume: 25, Issue No: 03, PP: 166-178, 2022.

[10].J.Mohamed Aslam and Dr. K. Mohan Kumar, "Enhanced Cloud Security Using Biometric Authentication", NeuroQuantology, e-ISSN: 1303-5150, Volume: 20, Issue No: 06, PP: 8201-8214, 2022.

eISSN 1303-5150

AUTHORS PROFILE

J.Mohamed Aslam, pursued Master of Computer Science from Bharathidasan University, Tiruchirappalli and received M.Phil Computer Science from Bharathidasan University, M.C.A from Anna University, Chennai. Currently doing Ph.D as a full time research scholar in PG and Research Department of Computer Science, Rajah Serfoji Government College (Autonomous), Thanjavur, Affiliated to Bharathidasan University, Tiruchirappalli, Tamilnadu, India. He is having 03 years of rich teaching experience. His main research work focuses on Cloud Computing security issues. He is published 03 research papers in reputed international journals.

Dr. K. Mohan Kumar received Master of Computer Science, PhD in Computer Science from Bharathidasan University, Tiruchirappalli, and M.Phil computer science from ManonmaniamSundaranar University, Tirunelveli, India. Currently working as Head in PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, Tamil Nadu, India. His main research work focuses on Network Security, Machine Learning, Deep learning, Cloud architecture and IoT. He has published more than 68 research papers in Scopus indexed and UGC CARE listed journals, 26 years of teaching experience, 20 years of Research Experience and produced 8 PhD scholars till date.