The Scientific Temper (2024) Vol. 15 (1): 1790-1798
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.1.30
https://scientifictemper.com/

RESEARCH ARTICLE

Enhancing security of cloud using static IP techniques

J. M. Aslam, K. M. Kumar*

Abstract

The user authentication and access control procedures for data stored on a cloud server encountered numerous security risks and concerns. Because critical company data should only be accessible by authorized workers, enhancing cloud security with static IP approaches is more beneficial. Even though the cloud providers maintain many security mechanisms, still the level of security should be raised by them due to lot of intruders who want to break their security mechanism. An encryption method is frequently used in most servers' security mechanisms. In this security mechanism, data in the cloud server may be stolen and misused. Security mechanisms using static IP addresses are another method for data security in cloud security. This paper explains that the static IP address security mechanism is better and more goal-oriented than that of earlier security systems.

Keywords: Cloud computing, Security mechanism, Authorized user, Internet protocol, Static IP, Dynamic IP, Cloud service provider.

Introduction

Cloud enterprises may take advantage of cost-effectiveness, scalability, and flexibility. The security of data stored on cloud servers is still a significant issue, though the increasing number of security threats and breaches has highlighted the need for robust user authentication and access to control mechanisms. Misconfiguration and malevolent common cloud security concerns. To protect sensitive corporate data in the cloud, adopting effective security measures that restrict access to only authorized people is critical. User authentication is an important aspect of cloud security. It validates a user's identification when seeking to access a network or computational resource. Password-based authentication all ways of user authentication. Because of these protections, there is a reduced chance of illegal access and data breaches because only authorized users can access cloud services. Traditional user authentication methods, on the other hand, have limitations and may not offer effective security against sophisticated assaults. Another critical feature of cloud security is access control. It governs who or what can access or use resources in a computer environment.

Good access control strategies guarantee that only individuals with permission can view particular information or carry out particular tasks. Traditional access control systems, on the other hand, have limits. Additionally, misconfigurations or insider threats can compromise the integrity and confidentiality of data. For example, they may not provide sufficient visibility over data flows, making identifying potential risks and vulnerabilities difficult.

Every Internet device has its unique IP address. The IP protocol in the routers reads the IP address specified in the data packets and directs to a destination IP address. If a user hosts a computer as a web server, the rest of the machines on the internet should be able to identify its IP address.

Static IP

Other computers' servers use the machine's static IP address to locate it. Internet service providers (ISPs) provide unique static IP addresses to every system that requires one. The ISP has agreed that the provided static IP address should not be utilized in more than one location. If they violate this agreement, the subscription will be raised. IPv4 or IPv6 static IP addresses are supported. In IPv4, all machines are not required to have a unique address. However, in IPv6, all machines are required to have a unique address.

Dynamic IP

However, each device within the hotel uses a dynamic address. Similarly, in a business network, individual devices

PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, (Affiliated to Bharathidasan University, Tiruchirappalli), Tamil Nadu, India.

***Corresponding Author:** K. M. Kumar, PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, (Affiliated to Bharathidasan University, Tiruchirappalli), Tamil Nadu, India, E-Mail: tnjmohankumar@gmail.com

How to cite this article: Aslam, J. M., Kumar, K. M. (2024). Enhancing security of cloud using static IP techniques. The Scientific Temper, **15**(1):1790-1798.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.1.30

Source of support: Nil

Conflict of interest: None.

Received: 15/01/2024 **Accepted:** 20/02/2024 **Published** : 15/03/2024

such as smartphones, streaming media players, tablets, and so on use dynamic addresses provided by the user network router.

Literature Survey

Mohamed Aslam J and Dr. Mohan Kumar K. (2022) explained numerous additional types of attacks, such as malware, phishing, and data theft, that always occur on cloud storage. This article looks at the percentage of various attacks and the damages they generate, and it finds that the most frequent type of attack is a data breach.

Mohamed Aslam J and Dr. Mohan Kumar K. (2022) discussed the encryption method prior to transferring data to cloud storage. This tactic can help reduce data leaks to some level. This study provides an appropriate client-side encryption method that improves cloud storage data security.

Mohamed Aslam J and Dr. Mohan Kumar K. (2022) evaluated cloud computing data kept on a remote server, raises a number of security risks and threat issues related to access control and user authentication. The latest biometric technology offers quick and easy authentication; it is unique. This study shows that biometric systems are more beneficial and goal-oriented than earlier recognition systems that relied on conjecture.

Mohamed Aslam J and Dr. Mohan Kumar K. (2023) discussed many security flaws and dangerous issues in the user authentication and access control mechanisms were found in the data kept on a cloud server. Because only authorized individuals should be able to access important corporate data, protecting it in the cloud is more valuable. Generally, security solutions employ encryption techniques. Another way to incorporate security features in cloud servers is through MAC addresses.

Raja Selvaraj and Manikandasaran S. Sundaram (2023) explained the cloud is the underpinning technology for all modern IT paradigms. Numerous programs run and save their data in the cloud. Businesses are interested in migrating their servers and data to the cloud to reap its benefits. Data security breaches are possible in the cloud due to its open, dispersed network architecture.

Sheena Edavalath and Manikandasaran S. Sundaram (2023) explained advantages such as utility service, on-demand service, portability, and flexibility make cloud computing appealing. The article presents an efficient cost-based resource allocation (ECRA) approach and framework to increase the efficiency and usability of resource allocation in heterogeneous cloud environments. No centralized resource allocation manager (CRAM) in a heterogeneous cloud can obtain all requested resources from a single counter. Resources are allocated via a cost-based mechanism.

Sheena Edavalath and Manikandasaran S. Sundaram (2023) explained, as previously, that the cloud is an intelligent technology that provides individuals with the services they have requested. It offers users an endless amount of benefits. Many small and medium-sized enterprises use cloud computing to establish and grow their operations. The users received the services after the requested resources were assigned. One of the most critical cloud duties is allocating resources efficiently and effectively.

Vani. K and Sujatha S. (2023) discussed The goal of this study is to systematize fault tolerance proposals, which will lead to a survey and the creation of a guided consultation environment for reading the relevant techniques for each case while also taking into account the variety of cloud computing environments and suggested approaches for treating fault tolerance in such environments. Systematizing suggested solutions aims to create a document that cloud computing system managers can use.

Materials and Methods

Traditional security mechanisms, such as data encryption, are commonly used to protect data stored on cloud servers. While encryption can provide a high level of security, it may not be enough to prevent data theft or misuse. Data in the cloud server can still be stolen and misused if the encryption keys are compromised or if the encryption algorithm is weak. Moreover, encryption does not address other security concerns, such as unauthorized access or misconfigurations. Therefore, there is a need for additional security measures that can complement existing encryption methods and enhance overall cloud security. One such security mechanism that can enhance cloud security is using static IP addresses with proper security measures in place. A static IP address can be as secure as a dynamic one.

The methodology for configuring a static IP address on a Windows 10 device is as follows:

- Open the settings window.
- Click on internet and network.
- Depending on your network connection, choose ethernet or Wi-Fi.
- In the local area connection section, choose properties.
- Select under IP assignment to make a change.
- Select manually enable the IPv4 button and enter the IP address.
- Enter the corresponding ISP's IP address, subnet mask, and default gateway.
- Select on save.

Three phases are recommended for system installation.

Registration of a New User

Figure 1 shows the process of creating a user of a new account is the first step. The user needs to enter their mobile number, email address, and name. After checking the information in the database, an OTP is issued to the user's cell phone. The user's account is created if the OTP is entered correctly. The user enters their mobile number, email address, and name.

- The system checks the database to see if the user already exists.
- The system sends an OTP to their mobile number if the user does not exist.
- The user enters the OTP and sets a password.
- The database stores the user's information.

Assigning Static IP to the Monitoring System

Figure 2 shows the second phase involves assigning a static IP address to a computer. The user must enter their username and password, and then an OTP is sent to their email address. If the OTP is entered correctly, the user is allowed to enter the static IP addresses of the computers they want to monitor.

- The user accesses the system.
- The system sends an OTP to their mobile number.
- The user inputs the OTP and confirms the number of computers to which static IP addresses must be assigned.
- The user enters each computer's static IP address.
- The static IP addresses are stored in the database.

Login Page for Those Who have Already Registered

Figure 3 shows the login page for already-registered users is the third phase. After users input their password and username, the system compares their static IP address with the database. The user can log in if the IP addresses match. The user's access is refused otherwise.

- The user logs in to the system.
- The system checks the database to see if the user's static IP address matches the one they are currently using.
- If the IP addresses match, the user is allowed to continue.
- If the IP addresses do not match, the user is denied access.

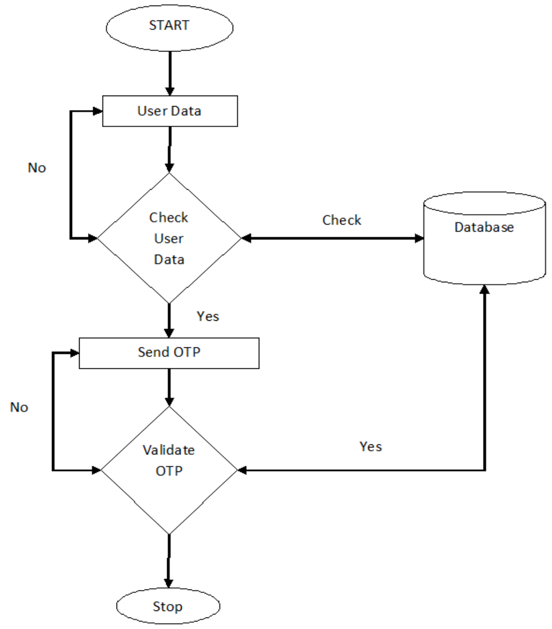


Figure 1: The new user registration flow diagram

The following are some of the benefits of using a static IP address:

- It provides a consistent IP address for a computer, which can be helpful for troubleshooting network problems.
- It can be used to set up port forwarding, which allows specific applications to be accessed from the internet.
- It can be used to set up a static DNS server, improving web browsing performance.

The following are some of the disadvantages of utilizing a static IP address:

- The static IP address will no longer be valid if the computer is moved to a different network.
- The computer may not receive a dynamic IP address if the DHCP server is down.

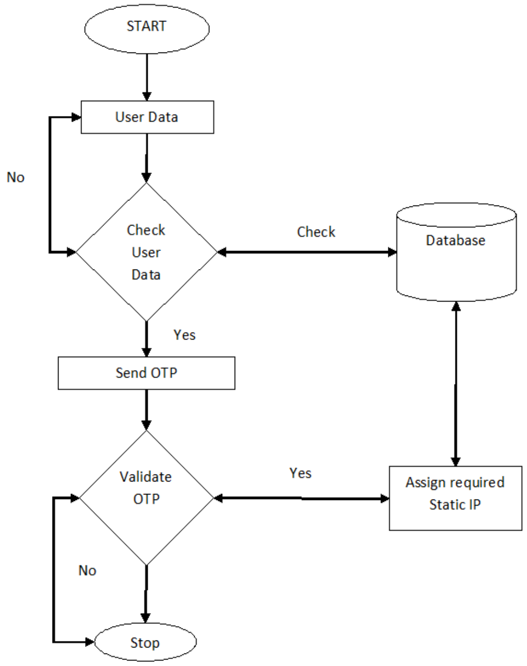


Figure 2: The flow diagram of static IP assigning

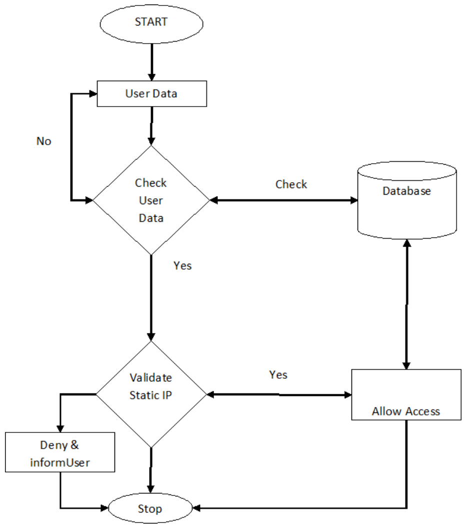


Figure 3: The flow diagram of existing registered users

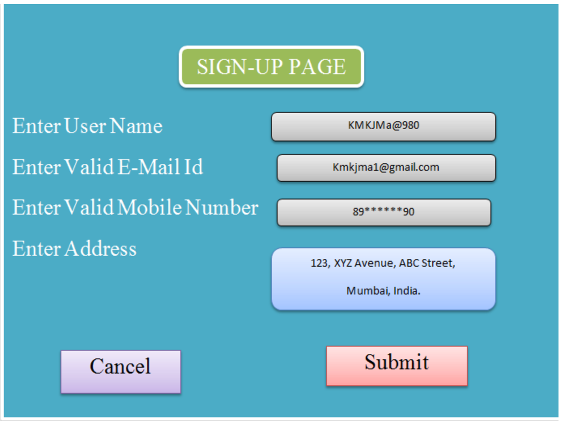
Overall, the benefits of using a static IP address outweigh the drawbacks. However, before selecting whether or not to utilize a static IP address for a particular computer, evaluate the pros and cons. This system prevents unauthorized access by requiring users to enter their static IP address when they log in. This ensures that only users granted access to the system can actually use it. This proposed system prevents unauthorized access to the monitoring system by requiring users to enter their static IP address when they log in. This ensures that only users to whom the system has assigned a static IP address can access it.

Results

Implementing the static IP address security mechanism involves assigning static IP addresses to authorized users or devices and configuring the cloud infrastructure to allow access only from those IP addresses. Only users with the designated static IP addresses can access the cloud resources. Monitoring and logging mechanisms can also be implemented to track and detect unauthorized access attempts or suspicious actions. Being proactive reduces the likelihood of data breaches and strengthens the cloud environment's overall security posture. User authentication plays a pivotal role in ensuring the security of cloud resources. While traditional user authentication methods have limitations, using static IP addresses can enhance the authentication process and provide an additional layer of protection. Assigning static IP addresses to VPN users using identity services engine (ISE), for example, can streamline the authentication process and ensure that only authorized users with designated IP addresses can access the cloud resources. Static IP addresses offer several advantages in terms of user authentication. Firstly, they provide fast connections, allowing efficient and seamless access to cloud resources. Secondly, static IP addresses simplify remote access, as the designated IP address can serve as a unique identifier for authorized users. This eliminates the need for complex authentication procedures and reduces the risk of unauthorized access. Static IP addresses offer enhanced stability as they remain constant over time. This stability ensures that the authentication process is reliable and consistent, further enhancing the security of cloud resources.

Furthermore, using static IP addresses for user authentication can provide increased manual oversight and control. Organizations can easily track and monitor user activity by associating specific users with static IP addresses. This allows for better visibility and detection of any unauthorized access attempts or suspicious activities. The use of static IP addresses in user authentication is a proactive approach that strengthens the overall security posture of the cloud environment.

The sign-up page (Figure 4) is clear and concise, and the instructions are easy to follow. The user must enter name, email address, and other necessary data.



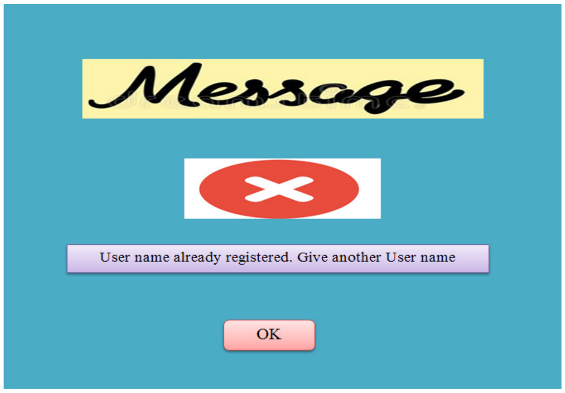
Enter User Name KMKJMa@980

Enter Valid E-Mail Id Kmkjma1@gmail.com

Enter Valid Mobile Number 89******90

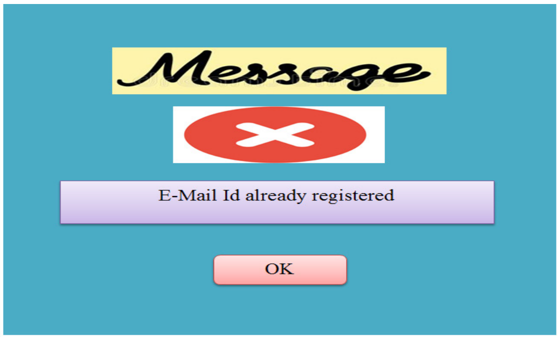
Enter Address 123, XYZ Avenue, ABC Street,
Mumbai, India.

Figure 4: Sign-up page of new user



User name already registered. Give another User name

Figure 5: User name already exists on page



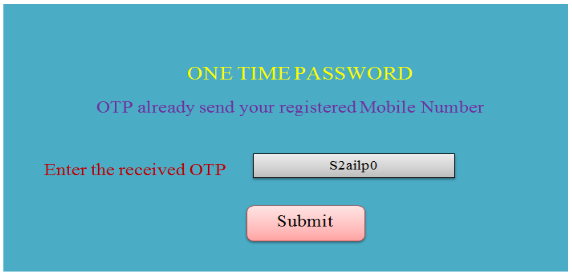
E-Mail Id already registered

Figure 6: Email Id already exist page

The user name already exists page (Figure 5) and the email ID already exists page (Figure 6) are informative and helpful. They let the user know that their username or email address is already in the database, and they provide instructions on how to proceed.

The OTP registration page for new users (Figure 7) and the creation of a new password page (Figure 8) are also clear and concise. They provide clear instructions on how to enter the OTP and create a new password.

The new user registration page (Figure 9) is a good summary of the user registration process. It shows the user the information they have entered and provides a link to the login page.

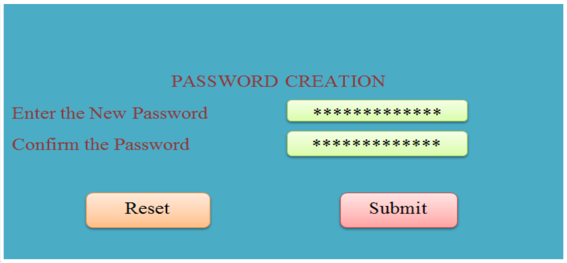


ONE TIME PASSWORD

OTP already send your registered Mobile Number

Enter the received OTP: S2ailp0

Figure 7: OTP Registration page for new user

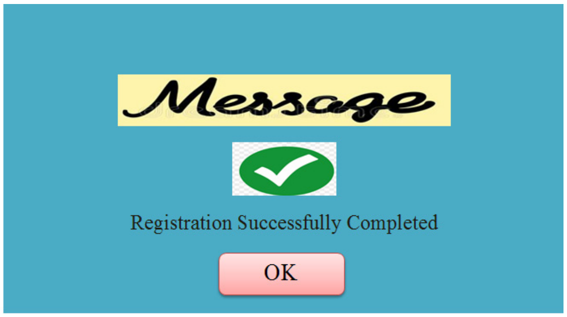


PASSWORD CREATION

Enter the New Password: *************

Confirm the Password: *************

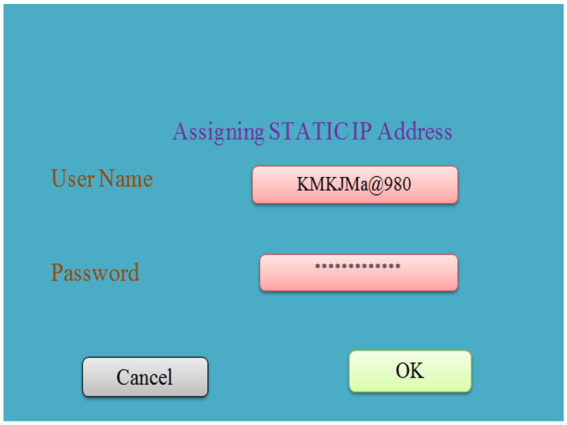
Figure 8: Creation of new password page



Message

Registration Successfully Completed

Figure 9: New user registration page



Assigning STATIC IP Address

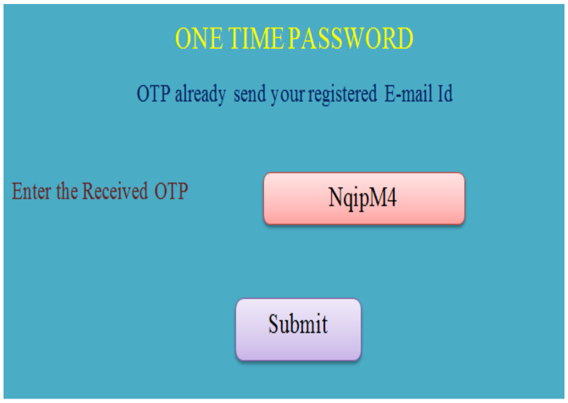
User Name: KMKJMa@980

Password: *************

Figure 10: Sign-in page for static IP address assigning

The sign-in page for static IP Address assigning (Figure 10) is clear and concise. It provides clear instructions on how to enter the OTP and assign a static IP address.

The OTP Registration page for static IP address assigning (Figure 11) is also clear and concise. It provides clear instructions on how to enter the OTP and assign a static IP address.

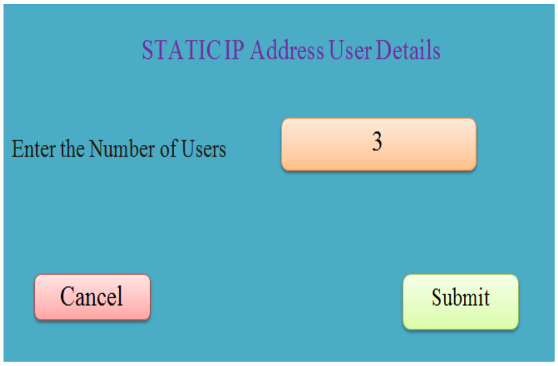


ONE TIME PASSWORD

OTP already send your registered E-mail Id

Enter the Received OTP: NqipM4

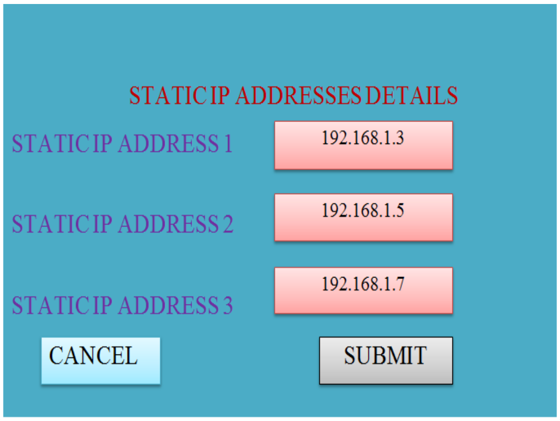
Figure 11: OTP registration page for static IP address assigning



STATIC IP Address User Details

Enter the Number of Users: 3

Figure 12: Enter the static IP address user details page



STATIC IP ADDRESSES DETAILS

STATIC IP ADDRESS 1: 192.168.1.3

STATIC IP ADDRESS 2: 192.168.1.5

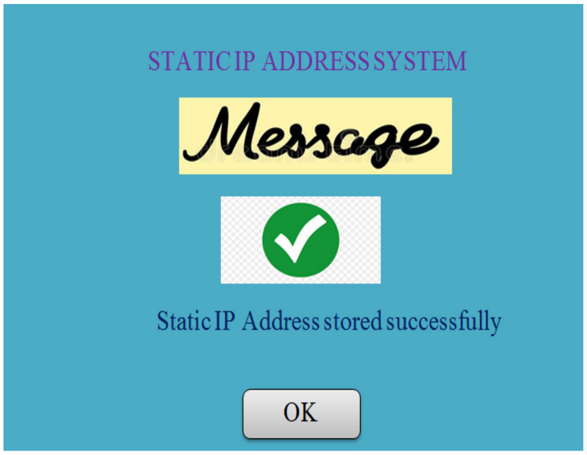
STATIC IP ADDRESS 3: 192.168.1.7

Figure 13: Enter the static IP address details page

Enter the address of the static IP user details page (Figure 12), which is informative and helpful. It provides clear instructions on entering the number of users who have registered the MAC address and a link to the next page.

The enter the static IP address details page (Figure 13) is clear and concise. It provides clear instructions on how to enter the static IP address details, and it provides a link to the next page.

The static IP addresses stored conformation page (Figure 14) summarizes the static IP address assignment process well. It shows the user the static IP addresses that they have entered, and it provides a link to the login page.

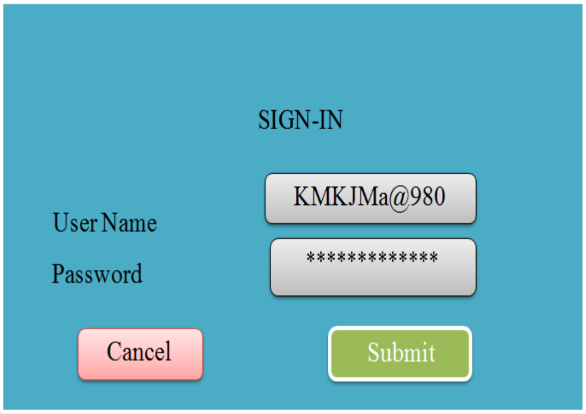


STATIC IP ADDRESS SYSTEM

Message

Static IP Address stored successfully

Figure 14: The static IP addresses stored conformation page

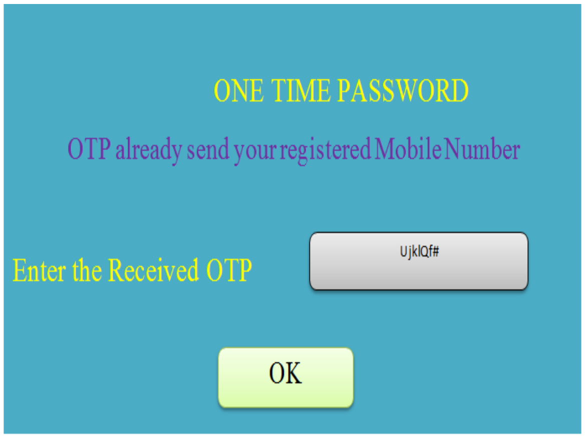


SIGN-IN

User Name KMKJMa@980

Password *************

Figure 15: Existing user sign-in page



ONE TIME PASSWORD

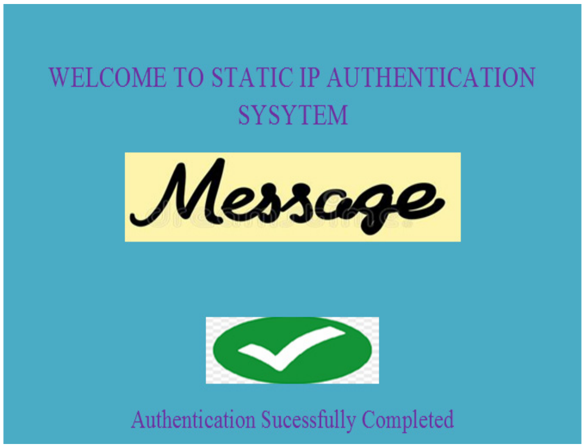
OTP already send your registered Mobile Number

Enter the Received OTP UjklQf#

Figure 16: OTP registration page for existing user

The sign-in page for existing user (Figure 15) is clear and concise. It provides clear instructions on how to enter the username and email address, and it provides a link to the next page.

The page where existing users register for OTP (Figure 16) is also clear and concise. It provides clear instructions on how to enter the OTP and login to the system.

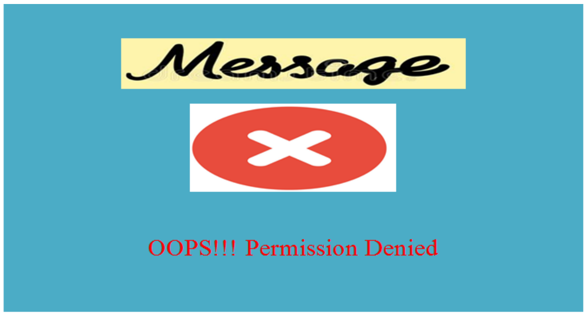


WELCOME TO STATIC IP AUTHENTICATION SYSYTEM

Message

Authentication Sucessfully Completed

Figure 17: The page of accessing allowed



Message

OOPS!!! Permission Denied

Figure 18: The page of access denied

The page of accessing allowed (Figure 17) is informative and helpful. It lets the user know they have been granted access to the system and provides a link to the main page.

The page of access denied (Figure 18) is also informative and helpful. It lets the user know that they have been denied access to the system and provides instructions on how to proceed.

Discussion and Analysis of Performance

The table provided shows the analysis of performance of several authentication methods. The methods are ranked in order of their success rate, with static IP authentication being the most successful and user name and password being the least successful. The following are some of the risks associated with each method:

User Name and Password

This method is the least secure, as it is susceptible to brute-force attacks and password spraying.

One Time Password

This method is more secure than user name and password but can be vulnerable to man-in-the-middle attacks.

Biometric Authentication

This method is very secure, but it can be expensive to implement.

Table 1: Analyzing performance with different approaches

S. No.	*Procedure*	*Risk types*	*Entire count of user attempts*	*% of sucesss rate of user*
01	User name and password	Weak or commonly used passwords	100	52
02	One time password	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
06	Static IP authentication	Access management	100	97

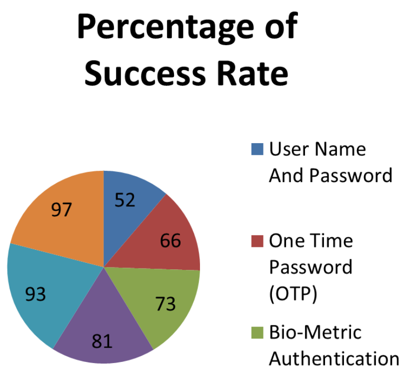


Figure 19: Pie diagram of performance analysis

URL Authentication Based

This method is relatively secure but can be vulnerable to phishing attacks.

MAC Address Authentication

This method is more secure than URL authentication, but it can be difficult to implement.

Static IP Authentication

This method is the most secure, as attackers find it very difficult to spoof a static IP address.

The success rate of each method is also affected by the number of user attempts. For example, if there are only a few user attempts, then a less secure method may still be successful. However, if there are a large number of user attempts, then a more secure method is more likely to be successful. Overall, the table shows that static IP authentication is the most secure method for authentication. However, it is important to note that no method is entirely secure. Consequently, to safeguard the systems, it is critical to deploy various security methods. Some further ideas on the table are as follows:

- The success rate of each method is based on a simulated attack. In a real-world attack, the success rate may be different.
- The number of user attempts is also a factor in the success rate. In a real-world attack, the attacker may try multiple methods or increase the number of user attempts.
- The table does not show the cost of implementing each method. The cost of implementation is also a factor to consider when choosing a security method.

The performance analysis of several techniques utilizing the online cloud-sim simulator is displayed in Table 1.

The performance analysis of Table 1 is graphically displayed in Figure 19.

Figure 19 shows the performance analysis of various authentication methods. The methods are ranked from least secure (User Name and Password) to most secure (Static IP Authentication). The figure shows that the success rate of users who use user name and password is only 52%. This is because hackers easily guess weak or commonly used passwords. A one-time password (OTP) is more secure than User name and password, but it is still not foolproof. If the cloud buckets are misconfigured, hackers can still gain access to the system. Biometric authentication is more secure than OTP but is not as widely available. URL authentication is more secure than biometric authentication, but it is still not as secure as static IP authentication. MAC address authentication is more secure than URL authentication, but it is still not as secure as static IP authentication.

Static IP authentication is the most secure authentication method because it is difficult for hackers to spoof a static IP address.

The figure also shows the types of risks associated with each authentication method. For example, user name and password are associated with the risk of weak or commonly used passwords. OTP is associated with the risk of misconfigured cloud buckets. Biometric authentication is associated with the risk of missing multifactor authentication. URL authentication based is associated with the risk of poor access management. MAC address authentication is associated with the risk of misconfigured cloud security. Static IP authentication is associated with the risk of access management.

Overall, the table shows that static IP authentication is the most secure method of authentication. It is also the most difficult method for hackers to spoof. However, it is important to note that no method of authentication is 100% secure. It is always important to take other security measures, such as using a firewall and antivirus software, to protect your system from unauthorized access.

Limitations

While static IP addresses can improve cloud security, issues and restrictions remain to be considered. One of the most challenging difficulties is updating the static IP address during a hacking incident. Once a static IP address is compromised, it becomes vulnerable to consistent attacks. This can be problematic as it limits the ability to respond quickly and mitigate security risks. Furthermore, an attacker can utilize a system with a static IP address as a springboard for other attacks if they can access it. Another limitation of static IP addresses is the potential for tracking and monitoring. Computers with static IP addresses are more accessible to trace than those with changeable IP addresses. This can concern organizations that prioritize privacy and want to prevent unauthorized surveillance or data collection.

Furthermore, managing static IP addresses can be challenging, especially in large-scale cloud environments. Assigning and maintaining static IP addresses for many users or devices can be time-consuming and complex. To ensure that each user or device is issued a unique static IP address that does not clash with existing addresses, meticulous planning and cooperation are required.

Moreover, the scalability of static IP address management becomes a concern as the number of users or devices increases. Despite these challenges and limitations, using static IP addresses in cloud security has proven effective in specific scenarios. Case studies showcasing successful implementations demonstrate the benefits of using static IP addresses. For example, organizations that restrict traffic to specific IP addresses at the firewall can leverage static IP addresses to enhance their security posture. This method provides fine-grained control over network traffic while reducing the risk of unauthorized access. Static IP addresses have several advantages over other cloud computing security solutions. They provide a more stable and reliable connection compared to dynamic IP addresses. This stability ensures consistent access to cloud resources and reduces the risk of disruptions.

Additionally, static IP addresses simplify remote access by serving as unique identifiers for authorized users. This eliminates the need for complex authentication procedures and enhances user experience. Looking toward the future, advancements in cloud security will continue to shape the effectiveness of static IP address security mechanisms. As software development evolves and programs are stored in locations other than the cloud, new approaches to security will emerge. Additionally, monitoring new cloud security trends and adopting best practices such as SDLC and DevSecOps will protect cloud environments from data breaches. The popularity and success of cloud computing will drive further advancements in information and communication technologies, leading to improvements in cloud security.

Conclusion

In conclusion, static IP addresses can significantly enhance cloud security by providing an additional layer of protection.

While there are challenges and limitations associated with static IP address security mechanisms, they can be mitigated through proper management and implementation.

Static IP addresses offer advantages such as stability, simplified remote access, and increased control over network traffic.

Organizations should evaluate the efficacy of static IP address security techniques as part of their overall security strategy as cloud computing expands.

By implementing stringent user authentication and access control procedures, organizations can enhance the security of their cloud resources and protect confidential information from misuse or illegal access.

Overall, the data indicates that static IP authentication is the most secure authentication method. It is also the most complicated way for hackers to spoof.

However, no authentication mechanism is entirely secure. You should always use additional security measures, such as a firewall and antivirus software to safeguard your system from unwanted access.

Acknowledgement

The Rajah Serfoji Government College Thanjavur, which is affiliated with Bharathidasan University, Tiruchirappalli, Tamilnadu, India, is to be thanked in the Department of Computer Science for the helpful support in using the computer science lab within the college.

References

Abdulsalam, Y.S. and Hedabou, M., (2021).Security and privacy in cloud computing: technical review. Future Internet, 14(1):11 Doi.org/10.3390/fi14010011

Bravo-Arrabal, J., Zambrana, P., Fernandez-Lozano, J.J., Gómez-Ruiz, J.A., Barba, J.S. and García-Cerezo, A., (2022). Realistic deployment of hybrid wireless sensor networks based on ZigBee and LoRa for search and Rescue applications. IEEE Access, *10*,: 64618-64637. Doi.org/10.1109/ACCESS.2022.3183135

Cardenas, M.M.,(2023). Mitigating Cyber Security Risks Posed by Self-Service Analytics (SSA) Tools : Creation of a Standardized Audit https://www.proquest.com/openview/78dfe9e41f0f293c7d728d885f3f3791/1?pq-origsite=gscholar&cbl=18750&diss=y

Forbacha, S.C. and Agwu, M.J.A., (2023). Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet). American Journal of Technology, 2(1):1-36 Doi.org/10.58425/ajt.v2i1.134

Fortino, G., Guerrieri, A., Pace, P., Savaglio, C. and Spezzano, G., (2022). Iot platforms and security: An analysis of the leading industrial/commercial solutions. Sensors, 22(6):2196 Doi.org/10.3390/s22062196

Ghelani, D., Hua, T.K. and Koduru, S.K.R., (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking Authorea Preprints https://d197for5662m48.

cloudfront.net/documents/publicationstatus/90319/preprint_pdf/87c34d475885f4f2b553401959b483cb.pdf

Mohamed Aslam J, Dr. Mohan Kumar. K (2022). Assessment of Security Attacks in Cloud", International Journal of Mechanical Engineering, ISSN: 0974-5823, Volume: 07, Issue No: 01: 2599-2606. https://kalaharijournals.com/resources/301-320/IJME_Vol7.1_314.pdf

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

Mohamed Aslam J, Dr. Mohan Kumar. K (2022). Enhanced Cloud Security Using Biometric Authentication, NeuroQuantology, e-ISSN: 1303-5150, Volume: 20, Issue No: 06: 8201-8214.

https://www.neuroquantology.com/media/article_pdfs/8201-8214.pdf

Mohamed Aslam J, Dr. Mohan Kumar .K (2023). Enhancing Cloud Security Using MAC Address, NeuroQuantology, e-ISSN: 1303-5150, Volume: 21, Issue No: 03: 120-140, https://www.neuroquantology.com/media/article_pdfs/120-140.pdf

Nakamori, T., Chiba, D., Akiyama, M. and Goto, S., (2019). Detecting dynamic IP addresses and cloud blocks using the sequential characteristics of PTR records. Journal of Information Processing:525-535 Doi.org/10.2197/ipsjjip.27.525

Raja Selvaraj, Manikandasaran S. Sundaram (2023). ECM: Enhanced confidentiality method to ensure the secure migration of data in VM to cloud environment, The Scientific Temper, ISSN: 0976-8653, Volume: 14 (3): 902-908. Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.53

Sheena Edavalath, Manikandasaran S .Sundaram (2023).Cost-based resource allocation method for efficient allocation of resources in a heterogeneous cloud environment, The Scientific Temper, ISSN: 0976-8653, Volume:14 (4): 1339-1344. Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.41

Sheena Edavalath, Manikandasaran S .Sundaram (2023). MARCR: Method of allocating resources based on cost of the resources in a heterogeneous cloud environment, The Scientific Temper, ISSN: 0976-8653, Volume:14 (3): 576-581. Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.03

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K., (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8): 4117 Doi.org/10.3390/s23084117

Usmonov, M., (2021). Basic Concepts of Information Security. Science web academic papers collection http://www.ijeais.org/index.php/home/

Vani.K , Sujatha.S (2023). Fault tolerance systems in open source cloud computing environments–A systematic review, The Scientific Temper, ISSN: 0976-8653, Volume:14 (3): 944-949. Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.59.

Yousefi, N., Alaghband, M. and Garibay, I., (2019). A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection, arXivpreprintarXiv Doi.org/10.48550/arXiv.1912.02629.