ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

Application Layer Model Focusing on DDOS and API Attack and Implementation of Multi-Factor Authentication Model

[1] Madhusudhan Devarapalli, [2] Ramakrishna Vankamamidi, [3] K.Sreeram, [4] Gonuguntla Koteswararao

[1] Senior Technical Specialist, Engineering and R&D Services, HCLTech
[2] Senior Solutions Architect, Engineering and R&D Services, HCLTech
[3] [4] Software Engineer, Engineering and R&D Services, HCLTech
Corresponding Author Email: [1] madhusudhanreddy-d@hcl.com, [2] rvankama@hcl.com, [3] k.sreeram@hcl.com, [4] gonuguntla.kotes@hcl.com

Abstract— The paper mainly focuses on the security issues in Application Layer and how it impacts the cloud .So we have walked through two top most attacks in this layer and what are the measures that could be taken in order to prevent or reduce them is our major goal, So a real-life example of these attacks have been discussed and the mechanism that could have stooped this attack have also been noted down , So by This we are able to conclude Multi-Factor Authentication lays down a solid platform to prevent these kind of attack .Hence a detailed version of an MFA Model has been proposed.

Index Terms: Cloud Security, Application layer, API Attack, DDOS Attack, Multifactor Authentication, MFA model Phishing Attack, Insecure API.

I. INTRODUCTION

Application-level security issues are a significant concern in cloud environments. Cloud computing offers numerous benefits, including scalability, flexibility, and cost savings, but it also introduces unique security challenges, especially at the application layer Hence focusing on application-level security issue in cloud is essential.

II. APPLICATION-LEVEL SECURITY ATTACKS

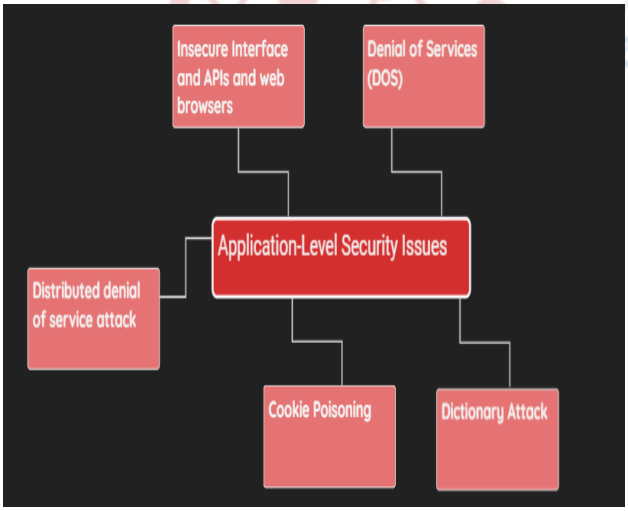

Fig.1. - [1]

Insecure APIs: Cloud provides an open platform for every user on the pay basis for how long they use. So, it provides a few interfaces and APIs to interact to the services provided to the user.

DOS: A situation where hackers flood a network server or web server with successive ask for services to damage the network.

DDOS: here an attacker tries to take down a computer or other device by interfering with its regular operation to prevent its intended users from using it is referred to as denial of service. Here the system is under the control of the attacker and the intended user's services are denied.

Cookie poisoning: It includes changing or altering the substance of a cookie to have unapproved access to a requisition or a site page. Cookies hold the client's personality-identified certifications and once these cookies are receptive.

Dictionary Attack: In a dictionary attack, the hacker makes utilization of all the conceivable word syntheses which could have been effectively used to decrypt the information flowing over the network.[1]

APIs- Abstract Application Programming Interface
DDOS -Distributed Denial of-Service

1. DDOS- (Distributed Denial of Service)

A denial-of-service attack is a kind of attack in which a malicious person tries to take down a computer or other device by interfering with its regular operation to prevent its intended users from using it. Here a target machine is saturated with a huge number of requests until normal traffic cannot flow through, which therefore denies the services of the user.[1]

2. HOW IT IS IMPACTING THE CLOUD

A DDOS assault can overwhelm a cloud provider's servers, making them unusable, or likely crash the provider's

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

entire system. Users who depend on the cloud providers' services may experience outages and service interruptions as a result. An enormous impact on other services and clients can result from a DDOS attack on a cloud provider.

Cloud providers frequently use tactics like LB, traffic filtering, and RB to lesser the impact of DDOS attacks. They might also make use of specialised real-time attack detection and mitigation DDOS protection services or equipment.[2]

LB -Load Balancing

RA -Rate Restriction

3. **DDOS Attacks experienced by industries**.

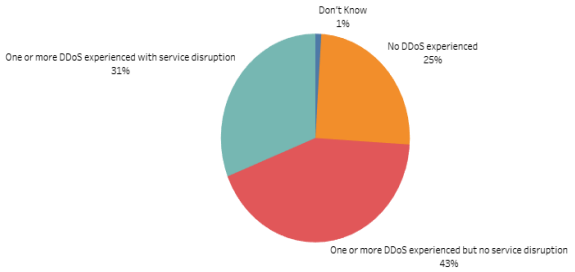

Fig. 2. - [2]

4. TOTAL DDOS ATTACKS IN MILLIONS, GLOBALLY, 2018-2013

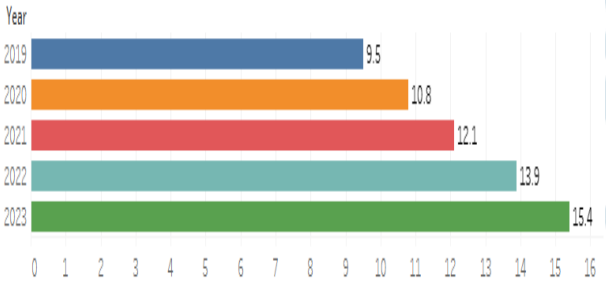

Fig. -3 - [3]

5. EFFECT OF CLOUD DDOS ATTACK

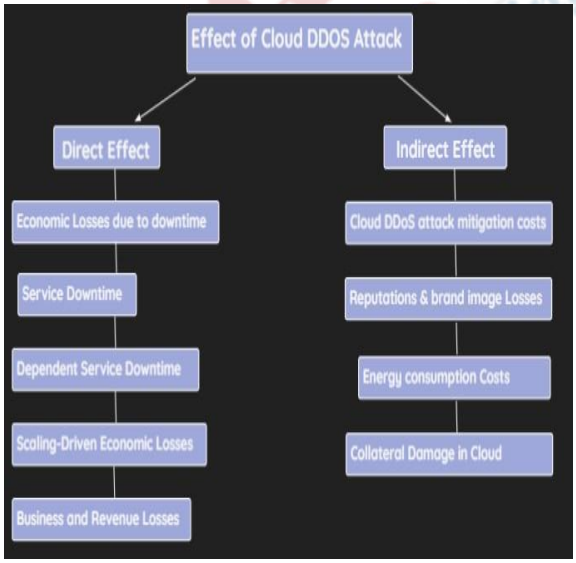

Fig. -4 [4]

6. CASE STUDY OF THE OPM DATA BREACH

This attack started in early March 2014 and went all the way up to April 2015. A botnet was used by the attacker to flood the website of the OPM with a large amount of traffic, therefore making the server slow for a long period, due to this the people with valid authorization were denied. On top of this, the attacker was also successful in stealing all personal data that were sensitive to the employees.[6]

This attack can be split into two parts. Here the first attacker was called (x1) and the second attacker was called (x2). (X1) was successful in stealing the manuals of IT Architecture and other kinds of information but in the initial phase, he was not able to access the personal records. An audit was conducted by USIS and Key Point (contractors) which led to a detailed background check and investigation on the workers who had access to the data as the main target of the attack started here.[7]

The second part of the attack started with the (X2) trying to access the networks on the website with the initial stolen credentials and injecting malware into the website and thereby creating a backdoor. They were too late to react to this attack even though they initiated what they call the big bang they were not able to get rid of the backdoor created by(x2). So, the breach stayed unnoticed and within Oct 2014 (X2) was successful in breaching the Department of Interior server that had many personal records of the employees.[8]

OPM- Office of Personal Management

USIS -United States Information Service

7. Aftermath of the OPM attack

A total of 21.5 million people data were stolen due to this attack, among them 19.7 million were government applicants and the other 1.8 million were the co-workers. Data such as Address proof, birthdates, pay histories, pension details, ages, gender, race, and fingerprints were among the stolen data. In consequence, Katherine Archuleta, the former OPM director, was forced to quit as an outcome of this attack. A 30-day security sprint to enhance and establish security procedures across all government organizations was another official response to the incident.[9]

8. MECHANISMS

There aren't many ways to stop this kind of attack. Utilizing two-factor authentication is one option. If someone logs into an account, the server will notify another device or source, allowing the account owner to confirm the login. The server responds by logging in to the user if the owner confirms the login. Because the account owner would have to approve the login before the user could access the account, using a 2-factor authentication system would have prevented unauthorized logins. OPM might have also changed the hacked Key Point login credentials to stop the data breach. The hackers were able to access OPM's Active Directory because of Key Point, preventing hackers from using the stolen credentials might have prevented the attack.[10]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

9. Key Controls for Prevention/Detection

The action regarding the security that the opm had to take in fixing the issues with the features represented below is quite necessary to prevent such kind of attacks from happening in the future they lacked strong authentication techniques and audit strategy needs to be implemented. Hence the following listed features are quite essential [10]

Features

- MFA
- Logging and Alerting
- RA

MFA-Multifactor Authentication

RA-Risk Assessment

10. INSECURE INTERFACE AND APIs

The interface is Insecure Application Programming Interface (API). Insecure Application Programming Interfaces having access to third-party applications by exposing the applications to Application Programming Interfaces may be required to leave their access credentials to third parties to enable their usage [11]. It's related to illegal authentication which leads to security issues for the application. Intrusion risks are higher in cloud resources which block visibility to network-based systems, especially accessing through the channel of insecure APIs [12].

11. HOW IT IS IMPACTING TO CLOUD

Insecure interfaces and APIs can have a significant impact on cloud security, as they can provide a pathway for attackers to gain unauthorized access to cloud resources.

Interfaces and APIs are the primary means by which users interact with cloud services, allowing them to manage and access resources such as data storage, compute power, and networking. In case these interfaces and APIs are insecure they can be exploited by attackers to gain authorization access to sensitive data or perform malicious attacks [fig A].

12. WHY?

A risk that relates to illegal authentication will lead to security issues happening in applications. Intrusion risks are higher in a cloud environment which blocks visibility to network-based systems, especially accessing through the channel of insecure APIs. Several root causes of most application security issues lead to bad applications. Such kind of cloud environments also use applications developed for in-house deployments therefore it causes more bugs. Hence, the insecure APIs cannot be underestimated [13].

13. Phishing Attack:

This starts with a cheating email or other way of communication that is designed to victim It just looks like comes from a trusted sender. If it fools the victim, the victim is tempted into providing confidential info. Sometimes malware is also downloaded into the target's device [14].

Attackers are getting a victim's credit card info or other personal data. These phishing emails are sent to employee login info or other details for use in an attack against a particular company. Its runs malicious code that triggers a malware download, which provides attackers with access to their device and any network to which connected devices. These attacks use different ways to communicate like email, text message, website, and pop-up.

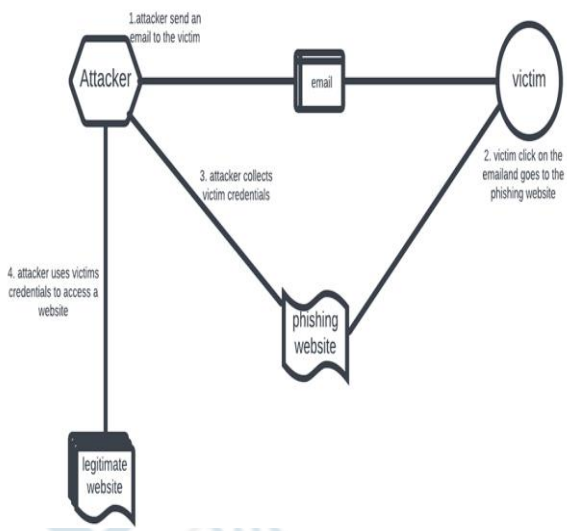

Fig 5: attacking process in electronic mail.

14. Case study:

Mahesh Bank got attacked by last year.

It is a Mahesh cooperative urban bank [15].

This issue happened in NOV 2021. The attacker sends 200 phishing emails to all the bank employees. They thought that these are normal spam emails because someone ignore the emails (these emails contain the (RTA) virus) but 2 of the employees click those links immediately attacker get access to enter the employee system, at that moment the connection was established. Then the attacker sends keylogger software (It's like whatever the employee does in the system everything knows by an attacker).

So regularly admin employee checks the customer account manually once done with their work they shut down the devices, The main mistake was all the master admins had the same domain name and passwords and they also had direct access to the bank database. At that time the attacker enters the device through login credentials they directly enter the bank server. The main reason is the whole process is going in one network and they were using weak firewalls and an old version of the operating system [16].

Because of their negligence in not providing of intrusion prevention system, intrusion detection system, or anti-phishing software. It's a huge cost of money for using this technology, but they approach the intra-soft company to provide security at a low cost for these measures. That's why this attack happen.

RTA- REMOTE ACCESS TROJAN

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

15. SUGGESTED MECHANISM

When we want an API to be secured, the general trend is to have different authentication techniques like passwords, etc to validate the identity of a user and to ensure that the authorized user accesses the cloud services [17].

1) When a new user registers at the API by filling in various fields like organization, name, designation, business need and tenant name else go to step (4) [fig B].
2) First, the API verifies whether the right tenant's name is entered and validates the employee's name against matching it with the employee id which is pre-stored in one of the servers at the cloud service provider end. If the validation is a success and the output is true go to the next step, else consumer's request is rejected, an alert notification will be sent to the tenant about an unauthorized attempt.
3) User is suggested to create and save a password for subsequent validation of tenant identity soon. Go to step (5).
4) If it is an existing user, the Password entered by the user will be validated by the API after computing its hash and matching it with the corresponding value precomputed and saved in a separate table. If authentication is true, go to step (5), else request is rejected, and a notification alert will be sent to the tenant about an unauthorized attempt.
5) API will permit a request if a legitimate user is accessing it. API validates the user's role once the user kept the tenant request and maps it with the activity, the tenant has been granted permission to work further.
6) If mapping is successful between the role and the respective activity, the user is approved and allowed by the API to perform the activity, else notification alert will be sent to the tenant about an unauthorized entry giving information about the phishing attack/employee.

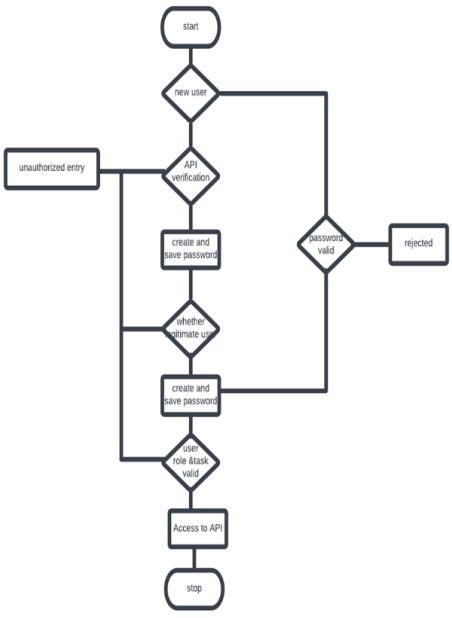

Fig 6: flowchart for valid authentication

Key components:

- Something you are aware of (password).
- Something you own (like text with a code sent to a smartphone authenticator app or another device).
- Something you're doing (biometrics using fingerprint, face, or retina).

16. Validation of OTP:

In the current scenario, many banks are providing authentication through the One Time Password (OTP) method which is generated through random under generation and used to verify the cloud user sometimes it is used for one-time authentication called system factor authentication. While sometimes it is used for two-time authentication called a Multiple Authentication Factor [fig c].

OTP -one time password

TWO TYPES OF OTP:

HOTP: It's a Hash-based one-time password, it is based on hash-based message authentication codes. The generation type of this code is based on a counter, that is activated and incremented with each event. These are valid until the code is requested by the user.

TOTP: It's a time-based one-time password, the duration of the timestep for TOTP is usually between 30 and 180 sec.

HOTP- Hash based one-time password.

TOTP- Time based one -time password.

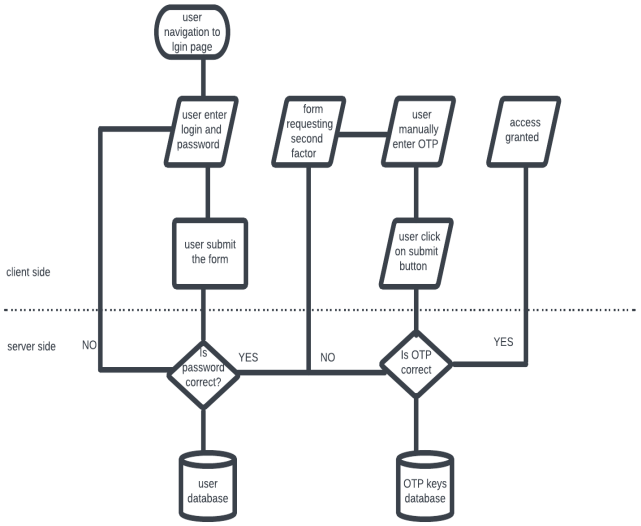

Fig 7 : verification process on client and server-side

III. FUTURE WORK

This analysis we follow up with Digital Multifactor authentication (MFA) is the best ways to make secure authentication. It covers many different areas of a Cyber-connected world, including online payments, communications, and access right management, etc. Most of the time, Multifactor authentication is little bit complex as it requires extra step from tenant. With this two-factor authentication, along with the credentials like user-ID and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

password, the tenant needs to enter a specific code which they normally receive by short message service [18].

Author (Roger Grimes) wrote an article about two-factor hacks three years ago, while more businesses are using more MFA methods to protect user credentials, and it still is far from universal. according to a survey by Microsoft last year (2021), 99.9% of compromised accounts (got attacked) did not use MFA at all and only 11% of enterprise accounts are protected by some MFA method.[19]

MULTIFACTOR AUTHENTICATION NEED FOR MFA

Businesses frequently utilize multi-factor authentication, to confirm that the visitors to their website are who they say they are. It is accomplished by giving at least two or more forms of identification confirmation. These pieces of evidence must belong to a different category, such as:

- anything they would only be aware of.
- something that they alone own.
- that which they are.

MFA operates in this way even if one of the factors is compromised by hackers there is a very small possibility that another factor will also be compromised or an unauthorized user. Due to the need for several factors for authentication [20]

HOW MFA IS USEFUL FOR BUSINESS

The main reasons to implement MFA in business are due to [21]

- Security
- Compliance
- Increase Flexibility and Productivity

VARIOUS WAYS TO IMPLEMENT MFA

Short message services

A short messaging service called SMS is used to finish this process, and it is activated during the login steps. A user is asked for a valid phone number to which a verification SMS can be sent when they register on a website along with the credentials. They must go through an additional identification check after setting up and verifying their phone number, during this period an SMS will be delivered to their verified phone anytime they log in to the website.[22]

Electronic mail

When a user connects to the website using their login information, a one-time unique code will be generated during this process, and it will be sent to their registered email address. The user will select the code from the email and enter it into the website or app. This will serve to validate the user.[22]

Push Notification

In this procedure, a push notification is sent to the user's phone, which contains your business app, when they enter the website using their credentials. The user will be automatically logged into their account after they approve access from the screen where this notification typically shows, which happens to be the main screen.[22]

Iris scanner

The iris of the user is scanned, and a database is used to safely store this data. The user must place the eye in front of the iris scanner. The system processes the iris image that was captured by the scanner. The database template and the recorded iris image are compared. To find a match, the algorithm examines the iris' patterns and properties.[23]

Fingerprint scanner

A fingerprint sensor is used to first scan a user's finger, which is then transformed to a digital template format. So, the first step is to gain access to a protected system. The system initially asks the user to place his fingers on the fingerprint sensor and the device takes a picture of the user's fingerprints. The saved fingerprint is now compared to the one that was captured. Because a fingerprint is unique to each person so it cannot be forged easily. Hence MFA adds an additional degree of protection by adopting a fingerprint authentication process.[24]

Multifactor Authentication Model [25] [26]

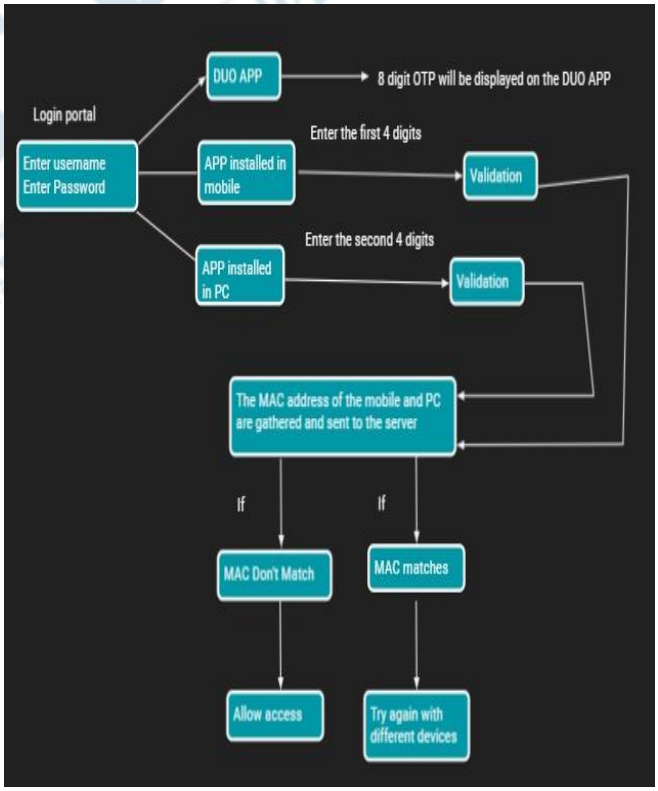

Fig-8.- [25] [26]

- First the user must enter his credentials, in this case its username and password, after successful validation the user moves on to the next stage which is the OTP validation.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

- Here an 8-digit OTP code is generated in the server, and it is sent to the app for displaying purpose, in this case we are using a DUO app.
- A secondary App is installed on both the user devices on which the user is going to enter his OTP for validation.
- The first 4 digit of the OTP displayed on the DUO app must be entered on the mobile phone and the second 4 digit of the OTP must be entered on the PC.
- The entered OTP is validated with the generated OTP, if matches then it moves to the next stage.
- Here we must make sure that the user is using two different devices for validation, So the MAC address of both the devices are compared.
- If MAC matches then we must deny the access, if the MAC are different, it is clear that the user has used 2 different devices, hence access can be allowed.

DUO- Security platform app

MAC- Media Access Control Address

FLOW CHART OF THE ABOVE MODEL

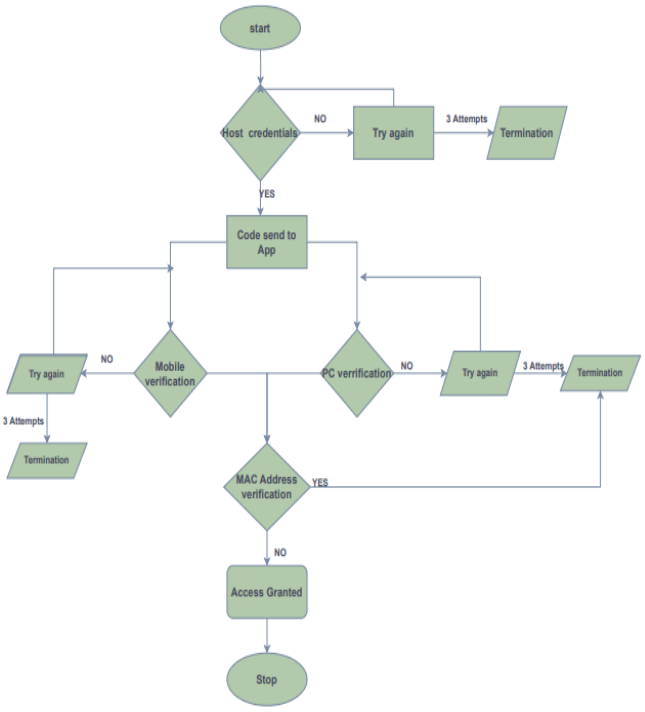

Fig-9

IV. CONCLUSION

In This paper, it's showing enhanced security mechanism to develop ourselves from the current 2FA to multi-factor model as it provides a solid platform to prevent unwanted intruders from affecting our system . Additionally, the related work provides further insights in the design and development of MFA Model according to are needs and requirements.

REFERENCES

[1] Security issues on different layers of cloud –[International journal for research &development in technology]-Vol -5, Issue-Jan-2016

[2] Understanding DDOS attack and its effect in cloud environment by ScienceDirect website -https://www.sciencedirect.com/science/article/pii/S187705091500754

[3] A10 Networks - https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

[4] Understanding cloud DDOS attack and Cloud based DDOS protection by Indusface

[5] DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION by Christos Douligeris and Aikaterini Mitrokotsa - https://www.cse.chalmers.se/~aikmitr/papers/ISSPIT03.pdf

[6] OPM Data Breach – Network Security News- https://asamborski.github.io/cs558_s17_blog/2017/04/20/opm.html

[7] Office of personal management data breach - https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

[8] The OPM Data hack explained : Bad security practices meet Chinas captain America – by josh fruhlinger

[9] OPM Aftermath -by Megan gates - https://www.asisonline.org/security-management-magazine/articles/2016/06/the-opm-aftermath/#:~:text=Along%20with%20having%20their%20Social,previous%20jobs%20was%20also%20stolen.

[10] OPM Attack by David kennel a detailed report

[11] Muhammad Kazim, Shao Ying Zhu, University of Derby, UK. "A survey on top security threats in cloud computing", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[12] Computing, "International Journal of Emerging Technology and Advanced Engineering" Volume 5, Issue 6", June 2015)

[13] https://www.infosecurity-magazine.com/next-gen-infosec/api-attacks-threat-vector-2022#

[14] Why cloud providers are top targets for phishing attacks - Cisco Umbrella.

[15] Nigerian arrested in Mahesh bank scam (deccanchronicle.com).

[16] CP CV Anand explains about Mahesh bank cyber fraud - TV9 - YouTube.

[17] Pan ford - Mitigation Techniques to Security Flaws in Cloud

[18] Sanjeet Kumar Nayak, SubasishMohapatra, Banshidhar Majhi. An Improved Mutual Authentication Framework for Cloud Computing. International Journal of Computer Applications (0975¯8887) Volume 52¯No.5, August 2012. pp: 36-41.

[19] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, ―A survey on multi-factor authentication for online banking in the wild,‖ Comput. Secur., vol. 95, 2020, doi: 10.1016/j.cose.2020.101745.

[20] Multifactor Authentication A beginners Guide by -Ashish Kumar Yadav- https://www.loginradius.com/blog/identity/multi-factor-authentication-a-beginners-guide/

[21] Why multifactor authentication is useful for your business -Blog by zoho- https://www.zoho.com/blog/directory/why-is-mfa-important-for-your-business.html#:~:text=Having%20MFA%20ensures%20legal%20compliance,%2C%20and%20customers'%20sensitive%20data.

[22] What are the different ways to implement MFA - https://auth0.com/blog/different-ways-to-implement-multifactor/
[23] What are Iris and retina scanner and how do they work - https://recfaces.com/articles/iris-scanner
[24] MFA with bio metric- https://www.bayometric.com/mfa-multi-factor-authentication-biometrics/
[25] Multifactor Authentication in cloud computing Chapter 5- https://idr-lib.iitbhu.ac.in/xmlui/bitstream/handle/123456789/1052/Chapter%205.pdf?sequence=13&isAllowed=y
[26] Multifactor Authentication model using fingerprint hash code and iris recognition by-Krishna Prasad K