MultiStage Authentication to Enhance Security of Virtual Machines in Cloud Environment

Anitha HM[1]
Department of ISE
BMS College of Engineering
Affiliated to VTU, Bengaluru, India

Dr.P Jayarekha[2]
Department of ISE
BMS College of Engineering
Bengaluru, India

***Abstract*—The adoption of cloud computing in different areas has shown benefits and given solutions to applications. The cloud provider offers virtualized platforms through virtual machines for the cloud users to store the data and perform computations. Due to the distributed nature of cloud, there are many challenges and security is one of the challenges. To address this challenge, verification method is implemented to achieve high level security in the cloud environment. Many researchers have provided different authentication mechanisms to safeguard virtual machines from attacks. In this paper, Multi Stage Authentication is proposed to overcome the threats from attackers towards virtual machines. In order to authorize and access the virtual machine, multistage authentication incorporating the factors like username, email id, password and OTP is carried out. Mealy Machine model is applied to analyze the state changes with factors supplied at multiple stages and trust built with each stage. Experimental results prove that system is safe achieving data integrity and privacy. The proposed work gives the protection against unauthorized users, provides secure environment to the cloud users accessing the virtual machines.**

***Keywords*—Authentication; multi stage authentication; one time password; finite state machine; mealy machine**

I. INTRODUCTION

In cloud environment, many users deploy the applications. These applications are accessed by several users. Dependability of users on the cloud is increasing day to day[1] as the investment is lesser. Hence cloud environment is prone to security issues[2]. Illegal access, misuse of data and assets hacking by the malicious users are some of threats that has to be addressed with more importance. Proper authentication has to be in place to safeguard against these attacks[3]. Traditional authentication mechanisms such as password-based login suffer with security problems. Password hijacking, stealing and phishing attacks[4] are some of the threats which create burden on cloud environment. Hence the resource access from the attackers has to be protected by good authentication.

Many well-known cloud computing environments such as Google, Amazon and Microsoft have already adopted the multifactor authentication. The major usage constraint is with respect to the users as they need to use the extra effort to login providing more factors. There is one more main concern to safeguard the user's credentials as they are shared with cloud environment to access the services from the cloud. Cloud users perform computations using virtual machines where they store the data and continue working till completion. Virtual machines belonging to different users are stored in the same host. Hence security of the virtual machine (VM) has to be taken care with almost importance. Before the VM is granted or accessed by the cloud user, authentication has to be carried out. Authentication [5] helps in proving the trustworthiness of the cloud users. Single factor authentication suffered with the problems such as if the user forgets the password and losing of password will completely avoid the legitimate user to access the resources in the cloud. Multistage Authentication (MSA) gives an additional layer of security to access the resources in the cloud and cloud provider is sure of extra security along with service level agreement. First step for cloud users is signing the service level agreement with cloud provider, next step is multistage authentication to access the cloud. Hence using this multistage authentication avoids attacks by the compromised users. There are advantages of choosing multistage authentication when compared with normal authentication such as increased security in the cloud environment and prohibiting the unauthorized users in to the system.

A. Motivation

The main objective of the paper is to protect the VMs in the cloud environment from illegal access and theft of data using MSA. MSA in cloud environment considers more than one factor from cloud users side credentials so that authentication is stronger. Even though the attacker tries with any one factor, gathering all the factors is not an easy measure to enter the system. MSA offers robust method of authentication cloud users and benefits with effective solution to the authentication. To provide high degree of security in the virtualized cloud environment and protect against several cyber-attacks that happen. Using multiple factors [6] provides an additional step towards accessing sensitive and confidential data stored in the cloud provider's domain. It is normally common that most of the users will accessing the virtual machines from the same host. Hence, it's the cloud provider's responsibility to meticulously provide the access to the virtual machines with appropriate authentication mechanism. Its observed number of incidents happening in the cloud regarding the data theft and DOS attacks.

Some of the research questions to be considered are:

- Access to the virtual machines in the cloud environment by the registered users without hassles.

- Will the MSA approach recognize the unauthorized users?
- The security features such as integrity, confidentiality and authenticity are achieved or not?

B. Contribution

The paper starts with theoretical concept of authentication, state machine to provide strong model to overcome illegal access and protect the virtual machines from attacks. The paper includes

- Authentication requirement and different authentication approaches with pros and cons are explored in the paper.
- Mealy Machine is presented to analyze the authentication process performed by the legitimate user to build the trusted environment and prevent the unauthorized user at all states.
- The approach uses MSA to allow users to access VMs for completing the tasks assigned by their organization.
- To protect every user's credential in the cloud provider's domain, robust MSA approach is applied guaranteeing the integrity and privacy.

This paper is organized as Section 2 gives background, Section 3 describes the related work, Section 4 presents the proposed approach, Section 5 gives the evaluation of the algorithm, Section 6 explains the results and discussions and Section 7 concludes the paper.

II. BACKGROUND

A. Traditional Authentication

Authentication [7] is a technique of proving the identity of the user in accessing the system by providing the details such as password and username. Traditionally single factor authentication was used to enter the system with an access card. It is observed that every user obtaining any services from any provider normally uses password-based authentication [3]. This password-based approach is usually used across different applications on hosts. Password is a widely accepted mechanism as it does not involve any major complications, users have to memorise the password and apply whenever the authentication is required. Passwords can be plaintext, combination of various characters involving special characters, numbers and so on. Users have suffered with many attacks due to weak passwords. There are cases where random passwords are selected and attackers can crack passwords. The different types of password attacks are dictionary attack, brute force attack, session hijacking and so on. Attacks disrupt the normal functioning of the cloud environment. The usage scenario of any environment is the users register for the service with certain password, which gets stored in the cloud server. Claimant has to provide the password in order to prove that he is authorized user. If the password matches with the stored password, then the claimant users are authenticated. The systems usually advice to choose the strong password.

B. Authentication

User has to prove that he is legitimate and this can be done using authentication. Usual methods are username and password to prove identity of the user. With the advancements in the security measures of any network, two factor and multifactor authentication [8] was applied to defend against illegal users.

Authentication avoids unauthorized access [5] to the sensitive information. There are all possibilities that the attacker gains access to virtual machines and tampers the information [9] stored, which leads to integrity threat.

There are five types of authentication mechanisms type [10] [11] [12].

- Password authentication: This method involves the password given by the users with a combination of characters, symbols and numbers. Users have to create strong passwords to avoid attacks. Many users keep simple passwords to avoid remembering long and cryptic passwords. Hence users are at the risk of password attacks.
- Certificate Authentication: User identity is confirmed by the digital certificate issued by the certification authority. The best example is Aadhar card to identify the user. Users provide the digital certificate when they are using the services or resources from the server. Once the server verifies digital certificate, user is decided as the legitimate.
- Biometric Authentication: User identification based on the biological characteristics of the user. Using the biometric factors, access doors or login to the system is granted in some of private firms. Biometric feature can be added as one of the factors with multifactor authentication.
- Token generated method: User credentials are maintained and users receive the tokens on one of the credentials. They provide the tokens to prove their identity.
- Multi factor authentication: Users add more than one factor to authenticate himself with server to access the resources. Multifactor authentication (MFA) can take more than one factor at the same time or multilevel. Due to this method of authentication, system is protected with various threats.

Among these different authentication [13] mechanisms multifactor authentication is applied as it is one of the most promising approaches. Multi factor authentication [6] mechanism defends against the attacks with extra care. Factor is the one which user provides to claim who he is. Suppose an employee enters the organization. He can enter the organization by swiping the card. How will the doors get to know that he is authorized person? It's because he has the smart access card which can be used for authentication. In this smart card, there is integrated chip which controls the access to the office environment. Normally chip stores the user

authentication data, user identification and data used by the users with respect to applications.

The different types of factors are collected [14] from the user to authenticate are:

- Knowledge factor: Aspects that users know like passwords. This factor is normally shared between the user and the provider. Once the user chooses the factor, it will be stored in the provider's database server and each time the user enters his factor, it has to be validated.
- Possession factor: Aspect that user has such as mobile phone or any other device. It can be the one-time password, smart cards or security tokens. If the user happens to lose the device, it is difficult to authenticate the legitimate user.
- Inherence factor: Feature that user is like biometric feature, voice or fingerprint. This factor is the one that the user is and the biometric factors are unique to each and every user.

Table I below represent the different factors which users are aware of to make use.

TABLE I. DIFFERENT FACTORS THAT ARE CONSIDERED FOR AUTHENTICATION

Knowledge factor	Possession factor	Inherence factor
User Knows- PIN, Password, security question related to his DOB or anything which user is aware of.	User possesses- Mobile phone, Smart card or tablet on which receives one time password(OTP), random password, etc	User is identified with biometric features: Iris, finger print or face recognition

The advantages of multi factor authentication [15] are:

- Improved Security: System security is enhanced by introducing the multifactor authentication. Additional Layers of authentication will add on to the security.
- Compliance: Necessary conditions of the organization are satisfied.
- Flexibility: Options for authentication is improved with more factors compared to traditional password authentication.

III. RELATED WORK

Ometov et al [15]., has discussed about multifactor authentication right from single factor authentication. They have explored different authentication methods, applications and challenges involved in implementing the multifactor authentication. The authors have identified operational concerns such as usability, robustness, integration and security. They have provided the benefits of MFA towards security. The authors have proposed the reversed approach in which the factors obtained from the users have secrets such fingerprint or pin. Considering n as sum and I factors with S_e secrets provided to them.

Factors and correspondingly secrets can be written as

I_1:S_{e1}

I_2:S_{e2}

..

...

I_n: S_{en}

Secrets are provided by the user to authenticate so that they can enter the system. Assume there are four factors and user forget any one factor to enter, then there is a trusted cloud party, which will aid to recover factor so that the user will be able to enter the system. Some of the biometric factors such as fingerprint, face change over the time, for which there is support by trusted party to update the feature in the database. There is decision policy which helps in deciding whether the user is authenticated or not.

B. B.Gupta et al [16], have proposed a model for access control based on the identity and mutual authentication using smart cards. The approach has five different phases right from the registration to authentication including updation of credentials. Hash functions are used towards the data. The approach mitigates unauthorized access, eaves dropping and single sign on with smart cards. It also defends against DoS attacks, fake identity and illegal use of smart cards.

C. Singh and T. Deep Singh [17] have proposed MFA with three levels based on the three levels of authentication. At the first level the login and password are stored with double encryption such as SHA-1 and AES. Second level of authentication uses the out of band authentication technique. After the first level, server provides the OTP to registered mail. User has to prove that he is legitimate by providing the OTP to the server. Third level user has to click certain number of images and buttons on the screen to get authenticated. The approach provides the protection against various attacks like man-in middle, brute force and password guessing.

A. Bhanushali et al [18], have given a good input about different authentication algorithms with respect to security, usability, space and storage. They have described the algorithms such as draw a shape, grid selection and déjà vu authentication algorithm based on the images. In order draw a secret, technique user is provided with a drawing and user has to reproduce same by redrawing. In grid selection the user is provided with small grid and needs to draw the pattern for authentication. Déjà vu is based on the seed value generated by the trusted server towards the user and at the time of authentication, user has to prove using this value. The inference provided by the authors is graphical based approach is better than the textual approach with respect to security.

Multilevel authentication [19] is presented by the authors to enhance security for electronic devices. Three levels of security checks are performed to authenticate the legitimate user. First level of security check is done with normal password. Biometric authentication is carried out in the second level. Last level of security check is performed by the accelerometer.

The proposed approach in the paper does not need any trusted third party and the interaction is between the cloud

provider and cloud user. There is no need for the user to go through the sequence of images with MSA approach.

Some users might not be well versed with drawings and user has to go with stages and provide input. Hence the proposed work is friendly to the users and provides security with features such as confidentiality and privacy. The approaches implemented by the various researchers along with the security parameters are given in Table II.

TABLE II. IMPLEMENTED AUTHENTICATION APPROACHES WITH SECURITY PARAMETERS

Authors	Description	Security Parameters addressed
Ometov et al[15]	Multifactor Authentication	Highlighted the operational concerns robustness, security and integration.
B. B.Gupta et al[16]	Smart Cart Authentication	Protection against unauthorized access, eavesdropping and DoS attacks.
C. Singh and T. Deep Singh [17]	MFA based on three level authentications	Defends man-in- middle, brute force and password attacks.
A. Bhanushali et al[18]	Survey about authentication algorithms	Graphical based approach provides better security.
A.Dinakar et al[19]	Multilevel authentication	Three levels of security checks for authentication.

IV. PROPOSED APPROACH

The objective of the proposed work is to implement secure access to the virtual machines using Multistage Authentication. In Multistage Authentication more than one factor is considered. As per the authentication mechanisms, using multiple factors, system is less prone to attacks.

A. Adversary Scenario

Attacks are possible from the attackers to gather the information stored in the cloud server [20]. Attacker might also try to spoof and access the VMs from the cloud provider. In the Fig. 1 shown below, legitimate users are the authenticated users and attacker [21] is the one trying to intrude the system. In normal authentication, login and password are used to provide the VMs. The traditional approach will give opportunities for attackers to damage the security features such as data integrity, confidentiality and availability [22].

A formulation is obtained for the minimization of attacks on the virtual machines with automata theory. The model used to realize the approach is mealy machine. Given below are the details of the state machine and use case of mealy machine.

B. Introduction to State Machine

State Machine is the machine which works based on the behavior of the system. The output of the system depends on the user's input. The machine which has finite number of states is known as finite state machine. Let us consider the simple example of tube light. When the user switches on the button, the state changes to on and otherwise it is off. There are two states in this machine namely switch on and switch off which is depicted in the Fig. 2.

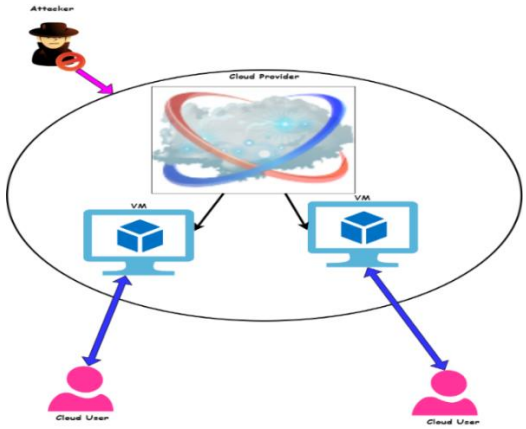

Fig. 1. Scenario of Risks.

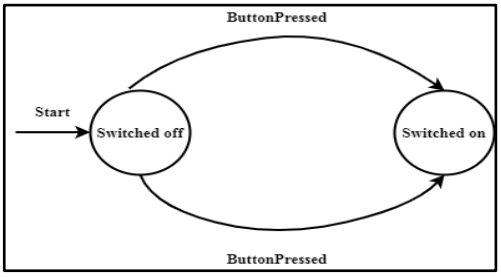

Fig. 2. State Machine of Tube Light.

C. Finite State Machine

Finite State machine is a computational model [23] with defined number of states. States always present the status of the system at the given instance. Consider the example traffic signal. As per the light shown, pedestrians cross the road and vehicles navigate through the traffic. This is one of the classic examples of Finite State machine. Finite state machine contains starting state, accepting states and final state. The output is either accept or reject. With specific input transition of state takes place. All these input symbols are represented in the alphabet.

Formal definition of finite state machine: It is represented with set of three entities shown in the equation 1:

$$F = (V, I, t_r) \quad (1)$$

V & I are non-empty finite groups

t_r: $V \times I \rightarrow V$ is a state transition function.

v_0: Initial state where $v_0 \in V$

I: input alphabet contains input symbols

To summarize the concept of the FSM as

- Has finite number of states
- Either zero or more accepting states
- Has at least one state
- Set of symbols for transition
- Has alphabet which has the set of input symbols.

Next followed by this topic, mealy machine is FSM depending on the present state and input symbol. The system is modeled with Mealy machine.

D. Overview of Mealy Machine

Mealy Machine is a finite state machine [24][25] in which output state depends on the current input symbol and state.

Let us find out (V, v_0, I, O, t_r, F):

V: Finite Set of States

v_0: Initial state

I: Set of symbols for transition

O: Output Symbol

t_r: Function of transition mapping V x I → V

F: Output function mapping to V→O

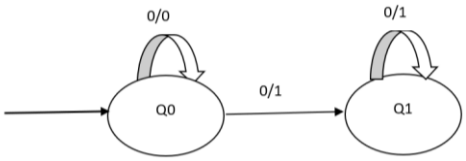

Fig. 3. State Transition in Mealy Machine.

Mealy Machine [25] has simple one input upon which transition to the next state shown in Fig. 3. Only two states are presented Q_0, Q_1. Input symbols are 0 and 1. Output is represented as 0 and 1. Mealy machines have fewer states compared to that of Moore machine. Mealy machines are secure to use; response for the inputs with mealy machines are faster. Mealy machines are used so that each level the trust is increased and only legitimate users are granted with the VMs.

E. Use case with Mealy Machine

The factors considered for the authentication are Email-id, password, Phone Number and One Time Password. Using mealy machine trust chain can be seen. In any of the stage the input is wrong, trust is broken. When the trust is broken by any of the user, it is very clear that it is the attack performed by the intruder. These factors are provided as the input symbols to the system. As per the factor and present state, the user progresses to the next state shown in the Fig. 4.

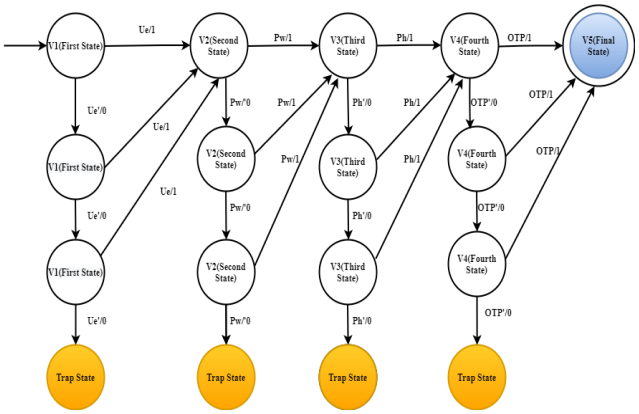

Fig. 4. Multistage Authentication System State Changes Depicted with Mealy Machine.

Here as per the input, the change in the state is seen. First user name and email id are the input symbol for state change. Next input symbol considered is password, followed by phone number and OTP. The system is multistage or multi-level where there are stages which legitimate user will be able to clear and succeed. Upon correct entry of email, password is generated to the valid email. User can login using the password generated. User has to go through the four stages in order to reach the final stage as shown in the Fig. 4. Every stage input and current stage important to advance to the next stage.

Let us represent the details of machine with the multifactor authentication

V= {V_1, V_2, V_3, V_4, V_5}

V1: Initial State or first state

I= { Ue, Pw, Ph, OTP}

O = {0, 1}

T_r is the transition function.

Upon receipt of matching symbols like email id, phone number, password and OTP, transition takes place to the next level in the system. The output states are 0 and 1. 0 represents failure and no transition and 1 depicting success along with transition to next state. Three attempts are considered in the proposed approach. As shown in the Fig. 4 the intruder at any stage tries to perform attack, cannot advance further and access the virtual machine.

F. Security Analysis with Mealy Machine

Attacks can be viewed and analyzed based[26][27] on the automata theory. The proposed MSA approach protects against attacks[28] which are discussed below:

- Replay Attack: If an attacker somehow gathers the email id and user name, guessing the secret password and gathering the OTP is not possible. Attacker cannot penetrate the cloud environment and access the virtual machines. With the mealy machine, if at any stage input is wrong, state change will not happen. Between V_1 an V_5, if the attacker tries to gather any factor and apply that in between randomly, successful authentication is not possible as mealy machine depends on current state also.
- Spoofing Attack: Attacker tries to impersonate in order to avail the virtual machines. Every time OTP is generated and it is not easy for attacker to get the OTP. There are multiple factors for attacker to guess, it is not just login and password compared to traditional systems. Intruder trying to capture *Ue*, *Pw*, User name and random password to authenticate himself is not accepted as password is received to legitimate user's email.
- Data theft resistant: The approach implemented overcomes the data theft as illegal access is not happening. If an attacker tries to intrude in any stage, there are only three attempts and third attempt being the last one, upon failure goes to trap state.

- Brute force attack: If any intruder tries to attack the system in any stage gathering some information, intruder cannot succeed in entering the system. As there are different levels and at each level if wrong input is raised, state change will not take place.
- Man in Middle attack: This system is resistant for man in middle attacks.

Intermediately in any state $V_i \in V$ where i→1,2,3,4,5 it is not possible enter the system. In order to validate the mealy machine model, simulation is performed and evaluated. The factors considered, algorithm steps and implementation details are presented below.

G. Methodology

Cloud user credentials are collected by the cloud provider during the registration phase. When users want to access the resources, authentication is performed. Here multistage authentication is used by the cloud provider. The factors considered for authentication in this approach are presented below.

- Email id: The user registers with his or her username and email ID. A unique hash code is created for each user using MD5 algorithm. MD5 algorithm [29] is used to encrypt the 4-digit random passwords generated for the user. The username and 4 digit non encrypted password are sent to the registered email ID. The user logs into his or her email account and must take note of the unique password provided in the body of the message. A link is sent to the registered email id. The user must click on the link included in the email to activate his account and get access to the login page.
- User name and password: Once the login page appears, the user enters the username and password sent via email. At this point they must also enter their contact number for the next level - OTP verification. If the username and password authenticate correctly, that is, if it matches with the information stored in cloud provider's database, the second factor is verified.
- One Time Password (OTP): Once the user clicks on the generate OTP button after providing the phone number, a random 5-digit OTP is generated and sent to the respective phone number. The user is required to enter the OTP. The entered OTP is verified with the temporarily stored OTP. If verification is successful, the user is granted access to the VM.

Multistage authentication shown in the Fig. 5 is explained step by step in the algorithm provided below. There are stages here in the approach. In the first stage, the email id and user name are provided. Cloud provider verifies in the database and sends the password to email. Using the password, user can login and provide the phone number for receiving OTP. This phone number is validated in the database and the OTP is sent. All these steps are shown in the Fig. 5.

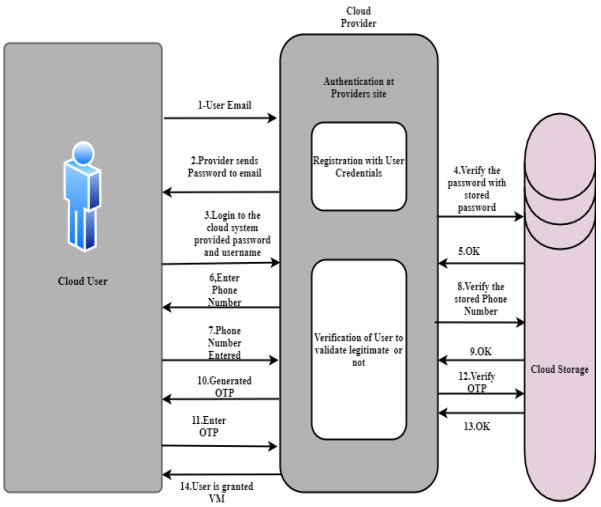

Fig. 5. Multistage Authentication Depicting Authentication Process.

Algorithm: Multi stage Authentication

Input: Username & Email-id

Output: Valid User is able to enter the cloud Environment

1. Begin
2. for each n users in the cloud provider Cp do
3. Enter Email-id Ue and User_name Un
4. Cloud Server Generates 4-digit password PW4 and sent to user's email-id Ue
5. Enter the user_name Un and Password PW4 in to the system
6. If (Un && PW4 with Cp server database)
7. Ask user to enter phone_no Ph
8. Send OTP to Ph
9. If (entered OTP == Cp Server Value)
10. Grant the user request
11. Else
12. Generate Alert to the Cloud Provider about illegal access
13. End

Notations used in the MFA approach are described in the Table III.

TABLE III. NOMENCLATURE OF THE TERMS USED IN THE PROPOSED MFA APPROACH

Notation	Description
Cu	Cloud user
Un	User Name
Rn	Random Number
Act. link	Activation link
Cp	Cloud Provider
Ue	User email id
PW4	Four-digit password
Ph	Phone number
OTP	One time password
H(.)	One way hashing
X->Y: A	Send A from X to Y

The stages of authentication are login, authentication and verification phase in order to grant user with virtual machines requested. This is depicted in the Fig. 6.

1) Login Phase

Step 1: Cloud user requests to allocate the virtual machine to the cloud provider with whom he is signed the SLA. Cloud user sends user name and email id.

Step 2: Cloud Provider generates four-digit hash and sends to the cloud user. Along with this activation link is also sent to the cloud user's mail id.

Step 3: User clicks the link to activate his account in the cloud environment.

2) Authentication Phase

Step 1: User enters the password provided by the cloud provider in to the cloud system.

Step 2: Cloud Provider asks the user to enter the valid phone number.

Step 3: Cloud User Provides the phone number.

Step 4: Cloud Provider generates the randomly five-digit password as one time password valid for 60 seconds to the cloud user's phone.

Step 5: Cloud User has to enter the OTP to access the virtual machine allocated for him by the cloud provider.

3) Verification Phase

Step 1: OTP generated is stored in cloud provider's database.

Step 2: Cloud User entered OTP is compared with stored OTP.

Step 3: Both are same, cloud user is granted virtual machine.

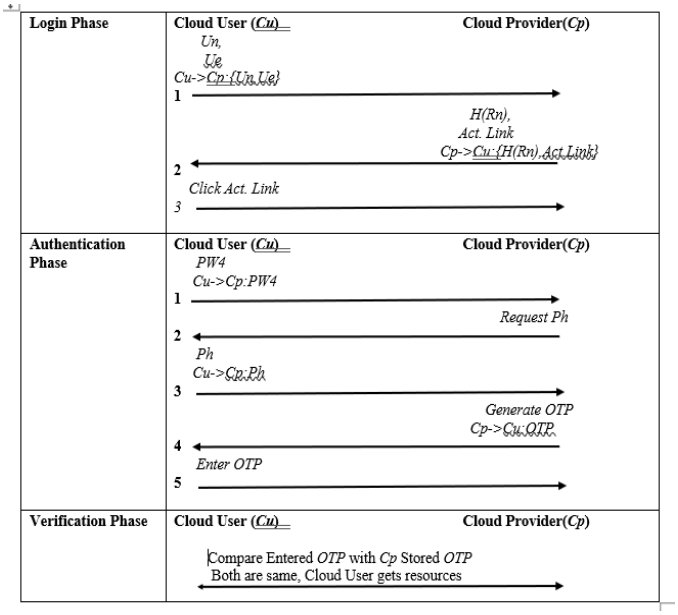

Fig. 6. Stages of Authentication.

V. Evaluation of Algorithm

Simulation is performed considering the many users and cloud provider. The authentication system is implemented using php, html and CSS at the front end, backend Mysql and XAMPP web server [30] solution stack. The backend database stores the user details. System has three modules viz. registering user credentials such as user name and email id, login page and OTP page. The algorithm has different factors for authentication. If the user is able to guess any of factor, it is not an easy mechanism for adversary to retrieve all factors. OTP is valid only for limited time and attacker breaking the OTP with in time duration is not easy. User has to sign up to access the cloud provider shown in the Fig. 7.

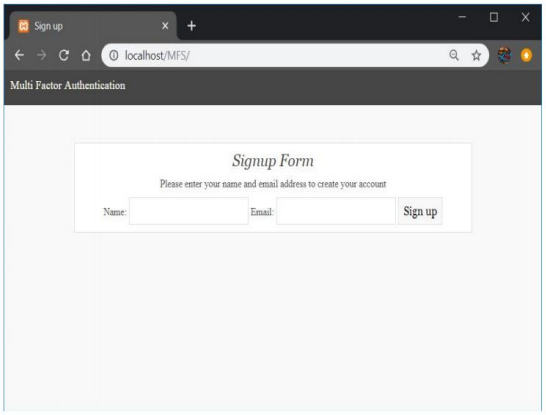

Fig. 7. User Sign up with cloud Server.

After the registration the username and unique password is sent to the user on his/her registered email id shown in Fig. 8.

Fig. 8. Reception of Username and Password by the user.

The user now knows his/her unique password and can access the login page, as shown in Fig. 9.

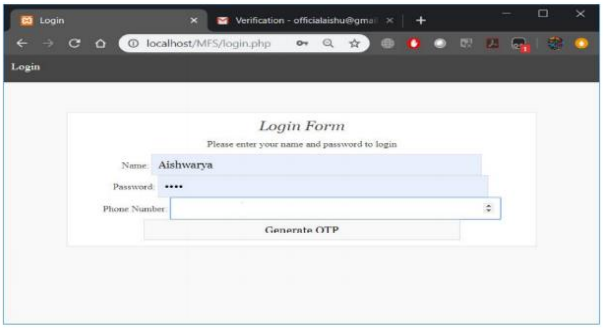

Fig. 9. Login Form.

Fig. 10. OTP Confirmation.

User receives the OTP on valid phone number and enters OTP as shown in Fig. 10.

When the user submits the OTP, it is verified with value stored in the cloud provider database and once it is confirmed the multistage authentication is complete. User has passed all authentication checks. Every time the OTP is generated and there is no chance of gaining the access to the cloud environment.

VI. Result and Discussion

Multistage authentication is checked for different time slots and recorded the successful attempts and failure attempts. In these number of successful logins is legitimate users. Testing is carried out using JMeter [31]. Login analysis is performed using JMeter. JMeter is opensource java-based tool used to test load and performance. Failure attempts some of them are intruders trying with brute force method to enter the system. The system is tested for the varying number of users right from 10 to 100.It is found that the system has provided resistance towards the attacks. Accuracy of system is calculated using the formula given below.

$$Accuracy = \frac{Sl}{Tl}$$

Where *Sl* is successful logins and *Tl* specifies total logins. The graph representation is shown in the Fig. 11.

The experiment is run for one hour, three hours and six hours. Overall Login statistics of users are depicted in Table IV.

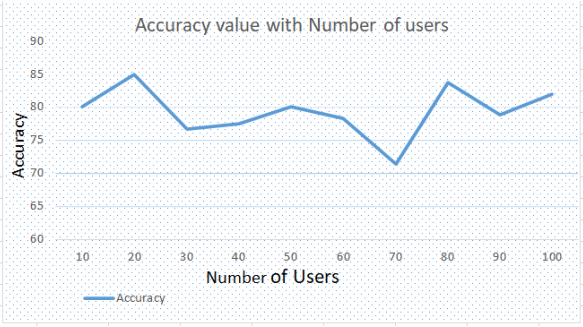

Fig. 11. Accuracy Depiction.

TABLE IV. Overall Statistics

Duration	60	180	360
Failure Login	33	42	77
Successful Login	63	88	95

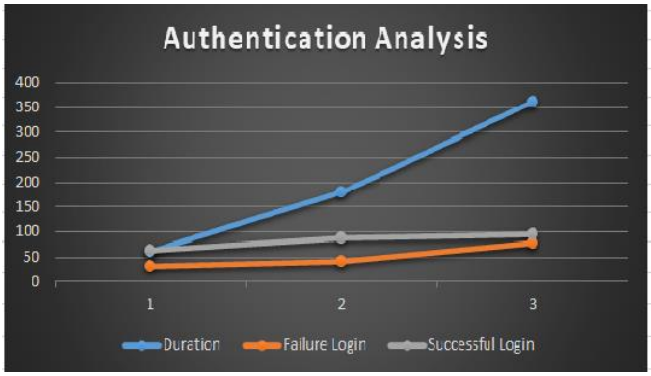

Fig. 12. Overall Login Statistics.

The graph in Fig. 12 indicates that MSA approach provides the legal access to cloud environment. The cloud users after the SLA contract with cloud providers can request for resources using MSA. MSA adds one more layer of security after SLA. The system does not allow the unauthorized access; hence approach provides privacy and protection against intruders who are trying to access the resources illegally.

VII. Conclusion

Cloud computing is technology which has lot of benefits to the cloud users in terms of cost, accessibility and scalability. Inspite of these advantages, there are many challenges and security is one of the challenges to be addressed. In order to protect against the attacks launched by illegal users, MSA mechanism is used in the applied. Different authentication mechanisms are discussed. Adversary scenario is presented and how attacker gains access to cloud resources to disrupt the regular functioning of cloud environment. The approach is validated with mealy machine theory. Mealy machine representation provides the stage changes along with trust flow from one stage to another to evaluate if any unauthorized access is carried out. MSA uses the factors viz user name, email id, phone number and OTP. Though user is registered, authentication mechanism has to be carried out every time user wants to access the virtual machines. The proposed approach protects against the attacks such as spoofing, replay and data theft. The results clearly depict how strong the authentication mechanism with respect to number of authenticated logins and time duration. With the observation of the approach implemented, it is quite unlikely to get the access by unauthorized users to the virtual machine which is meant for legitimate users. With the benefit of security, there is an overhead experienced by the user in passing through multiple stages to authenticate and access the VM whenever it is required.

In future, it is planned to consider the roles and grant the access to the virtual machines in cloud environment.

References

[1] G. Kaur and R. Kumar, “A Review on Reliability Issues in Cloud Service,” Int. J. Comput. Appl., no. Icaet, pp. 975–8887, 2015, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.1442&rep=rep1&type=pdf.

[2] R. Buyya, “Introduction to the ieee transactions on cloud computing,” IEEE Trans. Cloud Comput., vol. 1, no. 1, pp. 3–21, 2013, doi: 10.1109/TCC.2013.13.

[3] I. E. Liao, C. C. Lee, and M. S. Hwang, “A password authentication scheme over insecure networks,” J. Comput. Syst. Sci., vol. 72, no. 4, pp. 727–740, 2006, doi: 10.1016/j.jcss.2005.10.001.

[4] M. Kazim, “A survey on top security threats in cloud computing,” vol. 6, no. 3, 2015.

[5] N. Veeraragavan and L. Arockiam, “Enhanced Authentication Mechanism for Securing the Cloud Services using AaaS,” vol. 3, no. 3, pp. 171–175, 2016, doi: 10.17148/IARJSET.2016.3336.

[6] B. MacIej, E. F. Imed, and M. Kurkowski, “Multifactor Authentication Protocol in a Mobile Environment,” IEEE Access, vol. 7, pp. 157185–157199, 2019, doi: 10.1109/ACCESS.2019.2948922.

[7] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, “Authentication in cloud-driven IoT-based big data environment: Survey and outlook,” J. Syst. Archit., vol. 97, no. September 2018, pp. 185–196, 2019, doi: 10.1016/j.sysarc.2018.12.005.

[8] A. Acar, W. Liu, R. Beyah, K. Akkaya, and A. S. Uluagac, “A privacy-preserving multifactor authentication system,” Secur. Priv., vol. 2, no. 5, pp. 1–19, 2019, doi: 10.1002/spy2.88.

[9] A. Jesudoss and N. P. Subramaniam, “A Survey on Authentication Attacks and Countermeasures in a Distributed Environment,” Indian J. Comput. Sci. Eng., vol. 5, no. 2, pp. 71–77, 2014.

[10] Lal, Nilesh A., Salendra Prasad, and Mohammed Farik. "A review of authentication methods." vol 5 (2016): 246-249.

[11] W. Li and L. Ping, “Trust model to enhance security and interoperability of cloud environment,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5931 LNCS, pp. 69–79, 2009, doi: 10.1007/978-3-642-10665-1_7.

[12] D. D. Kumar, K. Vijay, S. Bhavani, E. Malathy, and R. Mahadevan, “A study on different types of authentication techniques in data security,” Int. J. Civ. Eng. Technol., vol. 8, no. 12, pp. 194–201, 2017.

[13] B. D. Deebak, F. Al-Turjman, and L. Mostarda, “Seamless secure anonymous authentication for cloud-based mobile edge computing,” Comput. Electr. Eng., vol. 87, p. 106782, 2020, doi: 10.1016/j.compeleceng.2020.106782.

[14] D. Dasgupta, A. Roy, and A. Nag, “Toward the design of adaptive selection strategies for multi-factor authentication,” Comput. Secur., vol. 63, pp. 85–116, 2016, doi: 10.1016/j.cose.2016.09.004.

[15] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, p. 1, 2018, doi: 10.3390/cryptography 2010001.

[16] B. B. Gupta and M. Quamara, “An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards,” Procedia Comput. Sci., vol. 132, pp. 189–197, 2018, doi: 10.1016/j.procs.2018.05.185.

[17] C. Singh and T. Deep Singh, “Article ID: IJCET_10_01_020 Cite this Article: Charanjeet Singh and Dr. Tripat Deep Singh, A 3-Level Multifactor Authentication Scheme for Cloud Computing,” Int. J. Comput. Eng. Technol., vol. 10, no. 1, pp. 184–195, 2019,

[18] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, “Comparison of Graphical Password Authentication Techniques,” Int. J. Comput. Appl., vol. 116, no. 1, pp. 11–14, 2015, doi: 10.5120/20299-2332.

[19] A. G. Dinker, V. Sharma, Mansi, and N. Singh, “Multilevel authentication scheme for security critical networks,” J. Inf. Optim. Sci., vol. 39, no. 1, pp. 357–367, 2018, doi: 10.1080/02522667.2017. 1374745.

[20] S. Milad Dejamfar and S. Najafzadeh, “Authentication Techniques in Cloud Computing: A Review,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 1, pp. 95–99, 2017, doi: 10.23956/ijarcsse/v7i1/01105.

[21] A. Ahmad, W. S. Zainudin, M. N. Kama, N. B. Idris, and M. M. Saudi, “State of the Art Intrusion Detection System for Cloud Computing,” vol. 10, no. 3, pp. 480–495, 2018.

[22] A. Narang and D. Gupta, “A review on different security issues and challenges in cloud computing,” 2018 Int. Conf. Comput. Power Commun. Technol. GUCON 2018, no. October, pp. 121–125, 2019, doi: 10.1109/GUCON.2018.8675099.

[23] N. Rasouli, M. R. Meybodi, and H. Morshedlou, “Virtual machine placement in cloud systems using Learning Automata,” 13th Iran. Conf. Fuzzy Syst. IFSC 2013, no. May 2019, pp. 7–12, 2013, doi: 10.1109/IFSC.2013.6675616.

[24] Aarts, Fides, et al. "Improving active Mealy machine learning for protocol conformance testing." Machine learning 96.1-2 (2014): 189-224.

[25] Mavridou, Anastasia, and Aron Laszka. "Designing secure ethereum smart contracts: A finite state machine based approach." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018.

[26] T. R. Thamburu and A. V. A. V, “International Journal of Advanced Research in A Survey on Trust Management Models in Internet of Things Systems,” vol. 7, no. 1, pp. 15–21, 2017, doi: 10.23956/ijarcsse/V7I1/0115.

[27] Q. W. Shang, K. Cao, and F. Wang, “The study on network attacks based on automaton theory,” Procedia Eng., vol. 23, pp. 653–658, 2011, doi: 10.1016/j.proeng.2011.11.2561.

[28] P. Kumar, “Cloud Computing: Threats, Attacks and Solutions,” Int. J. Emerg. Technol. Eng. Res., vol. 4, no. 8, pp. 24–28, 2016, [Online]. Available: www.ijeter.everscience.org.

[29] L. Khakim, M. Mukhlisin, and A. Suharjono, “Security system design for cloud computing by using the combination of AES256 and MD5 algorithm,” IOP Conf. Ser. Mater. Sci. Eng., vol. 732, no. 1, 2020, doi: 10.1088/1757-899X/732/1/012044.

[30] Mearaj, Insha, Piyush Maheshwari, and Maninder Jeet Kaur. "Data conversion from traditional relational database to MongoDB using XAMPP and NoSQL." 2018 Fifth HCT Information Technology Trends (ITT). IEEE, 2018.

[31] Shenoy, Srinivasa, Nur Asyikin Abu Bakar, and Rajashekara Swamy. "An adaptive framework for web services testing automation using JMeter." 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. IEEE, 2014.