SECURE AUTHENTICATION IN FOG COMPUTING

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology
in
Computer Science and Engineering/Information Technology

By
ABHINAV THAKUR (151282)
HARSHIT BHIMSARIA(151351)

Under the supervision of

DR. PRADEEP KUMAR GUPTA

to

Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled **" SECURE AUTHENTICATION IN FOG COMPUTING"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from August 2018 to December 2018 under the supervision of **(DR. Pradeep Kumar Gupta)** (Associate Professor, Computer Science Engineering).
The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Abhinav Thakur(151282)

Harshit Bhimsaria(151351)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

DR. Pradeep Kumar Gupta
Associate Professor
Department of Computer Science and Engineering, Jaypee University of Information Technology
Dated:

CONTENT

LIST OF FIGURES

LIST OF ACRONYMS & ABBREVIATIONS

OTP: One Time Password
PAC: Programmable Controller
APR: Address Resolution Protocol
NFC: Near Field Communication
APT: Advance Persistent Threats
ACI: Access Control Issues
AH: Account Hijacking
DOS: Denial of Service
STI: Shared Technology Issues
DL: Data Loss
IA: Insecure APIs
MI: Malicious Insider
SAV: System and Application Vulnerabilities
IDD: Insufficient Due Diligence
ANU: Abuse and Nefarious Use
DE: Data Breaches
TOTP: Time-based One-time Password
IIS: Image Identification Set
IBA: Image-based Authentication

ABSTRACT

We are aiming to develop a Secure Authentication in Fog Computing. Fog computing lies between the edge and the cloud network. It improves efficiency and reduce the amount of data transfer to the cloud network for analyzing, storing and processing. This is done to improve the efficiency and also for security. This project gives us various scheme which help in securing the data and implement multi-tier authentication. It first discuses about the problem in single tier authentication like Man-in-the-Middle and gives us an idea how we can prevent it by using multi-level authentication. The main objective of this secure authentication in fog computing is to understand and acknowledge the different type of authentication and implement them to secure fog platform and gives us more efficient performance and prevents security threats and help in more data storage.

CHAPTER 1

INTRODUCTION

1.1Introduction

Fog computing, otherwise called fog organizing or fogging, is a decentralized computing foundation in which information, process, stockpiling and applications are circulated in the most legitimate, proficient place between the information source and the cloud. Fog computing basically stretches out distributed computing and administrations to the edge of the system, bringing the points of interest and intensity of the cloud nearer to where information is made and followed up on. The objective of fogging is to enhance proficiency and decrease the measure of information transported the cloud for preparing, examination and capacity. This is regularly done to enhance effectiveness; however, it might likewise be utilized for security and consistence reasons. Prevalent fog computing applications incorporate shrewd framework, keen city, savvy structures, vehicle systems and programming characterized systems.

Fog computing is a promising computing worldview that stretches out distributed computing to the edge of systems. Like distributed computing however unmistakable attributes, fog computing faces new security and protection challenges other than those acquired from distributed computing. It very well may be depicted as a cloud-like stage having comparative information, calculation, stockpiling and application administrations, yet is in a general sense distinctive in that it is decentralized. Furthermore, Fog frameworks are equipped for preparing a lot of information locally, work on-introduce, are completely versatile, and can be introduced on heterogeneous

equipment. These highlights make the fog stage very reasonable for time and area touchy applications. For instance, Internet of Things (IOT) gadgets are required to rapidly process a lot of information. This extensive variety of usefulness driven applications strengthens numerous security issues with respect to information, virtualization, isolation, arrange, malware and checking. The larger part of fog applications is persuaded by the craving for usefulness and end-client necessities, while the security viewpoints are regularly disregarded or considered as a reconsideration.

A Fog framework has the accompanying qualities:

- It will be situated at the edge of system with rich and heterogeneous end-client bolster.
- Provide support to a wide scope of modern applications because of moment reaction capacity
- It has its own computing, stockpiling and systems administration administrations
- It will work locally (single jump from gadget to fog hub).
- It is exceedingly a virtualized stage.
- Offers economical, adaptable and compact organization as far as both equipment and programming.

Other than having these qualities, a fog framework is not quite the same as distributed computing in different angles and represents its own points of interest and weaknesses. A portion of the more Prominent are:

- A fog framework will have moderately little computing assets (memory, handling and capacity) when contrasted with a cloud framework, yet the assets can be expanded on-request.

- They can process information produced from different arrangement of gadgets.
- They can be both thick and inadequately circulated dependent on geological area.
- They bolster Machine-to – Machine correspondence and remote availability.
- It is workable for a fog framework to be introduced on low particular gadgets like switches and IP cameras
- One of their principle utilizes is as of now for versatile and compact gadgets.

Like Cloud framework, a Fog framework is made out of Infrastructure, Platform and Software-as-a-Service (IaaS, PaaS, and SaaS separately) alongside the expansion of information administrations. The Fog IaaS stage is made utilizing Cisco IOx API, which incorporates a Linux and CISCO IOS organizing working framework. Any gadget, for example, switches, switches, servers and even cameras can turn into a Fog hub that have computing, stockpiling, and system network. Fog hubs work together among themselves with either a Peer-to-Peer organize, Master-Slave design or by framing a group. The Cisco IOx APIs empower Fog applications to speak with IoT gadgets and cloud frameworks by any client characterized convention. For creating Fog applications in PaaS condition, Cisco DSX is utilized to make a scaffold between SaaS (Which really offers Metal-as-a-Service) and numerous sorts of IoT gadgets. It gives rearranged the executives of utilizations, computerizes approach requirement and backings different advancement conditions and programming dialects. The information administrations choose the appropriate place (Cloud or Fog) for information examination, distinguishes which information requires activity and expands security by making information unknown.

Numerous looks into and business foundation engineers trust that Fog stages will be created and discharged later on to give an improved and more solid framework to deal with the regularly expanding extension of associated computational gadgets. In any case, similarly as with every single conveyed framework, the introduction to digital dangers is likewise common and regularly elevated by the engineer's longing to give useful frameworks first, and afterward include safety efforts subsequently. Numerous explores are embracing a security-driven or secure by plan theory for delivering such conveyed frameworks. In any case, this perspective is still in its earliest stages and needs in thorough comprehension of the security dangers and difficulties confronting Fog framework.

While edge gadget and sensors are the place information is produced and gathered, they don't have the register and capacity assets to perform progressed examination and machine-learning assignments. In spite of the fact that cloud servers have the ability to do these, they are regularly too far away to process the information and react in an auspicious way. Furthermore, having all endpoints interfacing with and sending crude information to the cover over the web can have protection, security and lawful ramifications, particularly when managing touchy information subject to controls in various nations. In a fog situation, the handling happens in an information center point on a shrewd gadget, or in a brilliant switch or door, along these lines decreasing the measure of information sent to the cloud. Note that fog organizing supplements – not replaces – distributed computing: fogging takes into account present momentexamination at the edge, and the cloud performs assets serious, longer-term investigation.

1.1.1 Fog computing and Similar Technologies

In spite of the fact that the expression "Fog-computing" was at first settled by Cisco, similar ideas were examined and created by different gatherings. The accompanying rundown subtle elements three such advancements, including a portion of their atomic power contrasts.

1. Edge Computing: Edge Computing performs neighborhood handling on the programmable controller (PAC), which can confine preparing, stockpiling and correspondences. It represents an advantage of bicycling on the off chance that it restrains the purposes of disappointment and makes each gadget more free. A similar capacity makes it hard to alter and gather information in huge scale occupations, for example, IOT.
2. Cloudlet: Cloudlet is a center piece of 3-chain of command "cell phone - cloudlet - cloud". There are four critical qualities of Cloudlet: full restraint, has enough complex power, low end-to-end dormancy and based on standard cloud innovation. Cloudlet recognizes cycling messages and application virtualization isn't appropriate for the earth, merits more assets and can't work disconnected mode.
3. Micro-server farm: Micro-server farm is a little and completely useful server farm with numerous servers and is equipped for overseeing numerous virtual machines. Numerous specialized systems, including gynecology, can profit by small scale information insight, for example, loss of Latin, merit unwavering quality, moderately versatile, has regular security convention, split the data transfer capacity by pressure and can set up numerous new administrations.

1.2Problem Statement

Security dangers have been raised with the progression of cloud advances like malevolent insider assault, information misfortune and protection break. Security of distributed computing has turned into a noteworthy territory of research since most recent couple of decades. Cloud systems are defenseless against an assortment of assaults and security challenges. Cloud Server must recognize clients previously permitting them access to cloud assets. Validation plans are the key system to distinguish clients, which might be actualized through various strategies like secret word, biometric confirmation, open key foundation and symmetric key based verification plans. Security dangers are real hindrances in verification process in Fog Computing. Distinguishing proof of a client through single sign-on process like straightforward secret word based verification are never again thought to be secure i.e. they are shaky and helpless against assortment of assaults like Man-in-the-Middle assaults and lexicon based assaults. At the point when clients are permitted to pick their own passwords, they pick effectively recollect capable secret phrase and that can be effortlessly speculated. 75% individuals utilize same secret word for numerous assets and half of clients are hacked by means of phishing assault. Drop enclose secret key were hacked 2015 and client lost their privacy. In 2013, 44% of cloud specialist organizations lost their information because of savage power assault. Since 2011, security is taken as high need errand. A few creators recommend utilizing multi-level verification to enhance security framework. Multi-level confirmation plans are more secure than sign-on plans, as client needs to pass various strides previously getting to cloud assets. Distinctive multi-level validation plans exist that beat the shortcoming of single sign-on. The execution of existing multi-level validation plans is looked at into three parameters i.e. cost, ease of use and dimension of security.

1.2.1 Web Spoofing

One of the center man assault method is web caricaturing in which individuals were made to trust that they are cooperating with a confided in connection, however in real it's a shadow duplicate. The manner in which this assault works is extremely straightforward yet difficult to get away, the assailants brings the substance of a genuine site and copy the substance with a mock substance, which the client can't separate, which in the end result is spilling of some close to home data and information. One of the situations that clarify web ridiculing:

The aggressor parodied the client by a phony URL like the one which the client needs to access, by tapping on that interface, which the client needs to access, by tapping on that connect, which expressed as http://www.domain.com however in real it's alluding to a connection like hhtp://www.attackerdomain.org, when the client enters his id and secret phrase that will be put away in assailant's database for different pernicious exercises. Arrangement recommended is in this paper is "Believed Activity Chains". It's a structure level element that gives framework level resistance that can be influences by the application designers. This system expresses that every one of the means as well as projects should keep running in grouping. One action ought to be kept running anytime of time without enabling different exercises to keep running in parallel. A bolt is put on the running action by the framework to ensure a fruitful execution and fulfillment of that movement. When the movement is finished the following action in the continuous chain of exercises will be advanced for execution. This methodology ensures that any arbitrary or adhoc demand or action by the framework isn't executed specifically or in parallel while the exercises officially set in the chain are being run. The upsides of utilizing believed movement chain is securing

any mocking assault. At the point when exercises began, it oversees until the end which it expands unwavering quality. The huge issue of utilizing it when numerous exercises asked for in the meantime, It needs many intrude on bolt to deal with the majority of the exercises. It additionally impacts on execution that action not start until the point that the past action wrapped up.

1.2.2 APR Spoofing

Another sort of ridiculing exceptionally on neighborhood to recover activity is through (APR – Address Resolution Protocol). In APR satirizing the assailant send a mock message on system with intend to relate his MAC address with host IP address, so the activity will be redirected to the aggressor rather to the real client. The arrangement given in the paper to stop the APR mocking assaults is utilizing the "Open Stacks". It is open source cloud stage that utilizes part called correlation handler to solid APR tables developed in cornerstone. This guarantee the credibility of the tables and along these lines disposes of any bungle that occurs among messages and table. The unwavering quality expanded when table contained IP and MAC address and contrasted and each message it coordinated or expelled it. The issue is over-burden when APR tables contained numerous IP and Mac address contrasted and each message that got.

1.2.3 Why Fog Computing?

- As a center layer between end gadgets and cloud for computing can give extra highlights as an expansion of distributed computing to enhance information execution with different properties.

- Heterogeneity: with expanding danger of information security when straightforwardly getting to conventional distributed computing server farms, fog computing server farms, fog computing gives a virtual heterogeneous stage comprising of computing, stockpiling and systems administration benefits as an interface between end gadgets and genuine cloud server farms.
- Supporting endpoints with administrations at system edges because of mindfulness and low idleness in fog computing.
- Fog computing conveys the administrations and applications through intermediaries and passageways.
- Fog computing underpins portability which empowers the applications that are bolstered by fog to be spoken with cell phones straightforwardly.
- Real-time cooperation in fog computing can be utilized in vital applications that require constant association as opposed to bunch preparing.
- Fog is a type of cloud that keeps out of sight on or close ground level.

1.2.4 Authentication issue in Fog

The primary security issue in fog is validation since administrations are given to the end clients by front fog hubs. Numerous verification procedures connected for fog computing to give a productive confirmation yet some of them not effective and have poor adaptability, for example, customary PKI-based. Likewise, biometric validation methods connected to give an effective confirmation, for example, confront verification, unique mark verification, contact based validation or keystroke-based validation.

As referenced in, we have to apply an interruption location framework to each layer to keep any assault. One of the average assaults in fog computing which we center to discover as answer for it in this exploration is Man-in-the-Middle assault. Man-in-the-Middle assault is supplanting the portals that serving the fog gadget by phony one which is interfacing with malignant passageways. For this situation, any private correspondence of unfortunate casualty will be hacked and in this way the entryways will be controlled by the assailants. The aggressor will have the capacity to screen and adjust the information between end client and door. Customary strategy faces challenges to recognize fundamental in-the-center assault without perceptible highlights of this assault gathered from the fog since this assault expends a little measure of fog gadgets, for example, memory and CPU utilization.

1.3Objective

With the progression of innovation, there is an enormous need of solid verification plans. Scientist proposed diverse multi-level and multifaceted validation plans to give solid security to distributed computing systems. Some multi-level confirmation plans utilize one-time secret key while others depend on biometric filter, QR code or graphical example. A portion of the multi-level validation plans are:

- One-time Password (OTP)
- Smartphone for Authentication
- Risk based Authentication
- Biometric Authentication
- Graphical Password
- Smart-card based Authentication

- 3D Password
- Sequence of Activities
- Multilevel Authentication

What we propose is a new authentication scheme formed using a combination of techniques derived from the pre-existing techniques on the basis of comparison done between these techniques as a part of our study.

1.4Methodology

The customary and most seasoned technique for giving validation is utilizing usernames and passwords. The majority of the sites utilize this strategy to give security to their customer's close to home information. The username is utilized to distinguish which online record does client or customer needs to access and passwords are utilized to demonstrate the personality of that authentic client. Passwords are put away on server side in encoded structure or utilizing hash capacities, additionally the username and passwords transmit in scrambled structure over the safe association. Subsequently if any interloper get access over the system, there is no stress over spillage of significant data as it won't uncover any data about real secret word.

Despite the fact that it looks secure however in useful it isn't as secure as an assailant can get unique secret key of a customer utilizing savage power assault after a couple of blends. Additionally, the client keeps on utilizing simple and guessable passwords, so it is prescribed to utilize complex passwords or transforming it over and again after brief time of times. These single static passwords are likewise entirely defenseless

against social designing for example individuals may request passwords or can likewise figure them accurately. Some studies completed on different spots have uncovered that that it is so natural to get individuals uncover their passwords all around effectively. Any aggressor can likewise utilize these passwords to get to their own records else one has to change their passwords more than once. A couple of accentuation have been given on utilization of complex passwords like it's length ought to be least 8 characters, ought to have somewhere around one numeric and one uncommon image and so forth. In any case, because of different vulnerabilities and assaults like phishing, man in the center assault, animal power and so on static passwords, a need of solidifying the security of online information and data put away by the clients has been raised. Accordingly, after a couple of inquires about in the field of online security, a strategy has been proposed. In which the verification of genuine clients must be performed not just in a solitary advance through a secret key however is to be performed in different strides by requesting more data about the client by the server. This offers ascend to the presentation of Multi-step or Multi-factor confirmation conspire:

- **Username and Password**

The customary and most seasoned technique for giving validation is utilizing usernames and passwords. The majority of the sites utilize this strategy to give security to their customer's close to home information. The username is utilized to distinguish which online record does client or customer needs to access and passwords are utilized to demonstrate the personality of that authentic client. Passwords are put away on server side in encoded structure or utilizing hash capacities, additionally the username and passwords transmit in scrambled structure over the safe association. Subsequently if any interloper get access over the system,

there is no stress over spillage of significant data as it won't uncover any data about real secret word.

Despite the fact that it looks secure however in useful it isn't as secure as an assailant can get unique secret key of a customer utilizing savage power assault after a couple of blends. Additionally, the client keeps on utilizing simple and guessable passwords, so it is prescribed to utilize complex passwords or transforming it over and again after brief time of times. These single static passwords are likewise entirely defenseless against social designing for example individuals may request passwords or can likewise figure them accurately. Some studies completed on different spots have uncovered that that it is so natural to get individuals uncover their passwords all around effectively. Any aggressor can likewise utilize these passwords to get to their own records else one has to change their passwords more than once. A couple of accentuation have been given on utilization of complex passwords like its length ought to be least 8 characters, ought to have somewhere around one numeric and one uncommon image and so forth. In any case, because of different vulnerabilities and assaults like phishing, man in the center assault, animal power and so on static passwords, a need of solidifying the security of online information and data put away by the clients has been raised. Accordingly, after a couple of inquiries about in the field of online security, a strategy has been proposed. In which the verification of genuine clients must be performed not just in a solitary advance through a secret key however is to be performed in different strides by requesting more data about the client by the server. This offers ascend to the presentation of Multi-step or Multi-factor confirmation conspire.

- **One-time Password(OTP)**

OTP can be executed utilizing different systems and legitimate for brief day and age and can be utilized for one login session. Cloud administrations and assets are arranged into three dimensions i.e. low, medium, and abnormal state. This plan utilizes math captcha, OTP and IMEI number of enlisted for confirmation.

1. Low level authentication: Low dimension confirmation depends on username, secret key and number juggling captcha and client is allowed access to utilize low dimension assets.
2. Medium level authentication: notwithstanding client name, secret word and math captcha, one-time password (OTP) for getting to medium dimension cloud assets and administrations.
3. High level authentication: This dimension utilizes every one of the three elements for confirmation. First is number-crunching captcha, second is OTP and third is IMEI of enlisted cell phone. IMEI is partitioned into little lumps of two digits and request that client give three arbitrary fragments. On confirmation client is allowed full access to all cloud assets and administrations.

Securing OTP by adding another security layer to ensure identity of the user. User proves his identity by providing his personal information previously registered with system i.e. mobile number, IMEI and PIN to receive OTP. Single mobile number and IMEI can't be associated with multiple accounts. Strength of this scheme is that if hacker manages to get username and password and steals configured mobile, still unable to access user's account but extra hardware is required for sending OTP and IMEI is also not very secure as it is known to mobile network operators.

Image based OTP (imOTP) proposed in requires out of band channel for sending imOTP on smart phone which is pre-registered with cloud server.

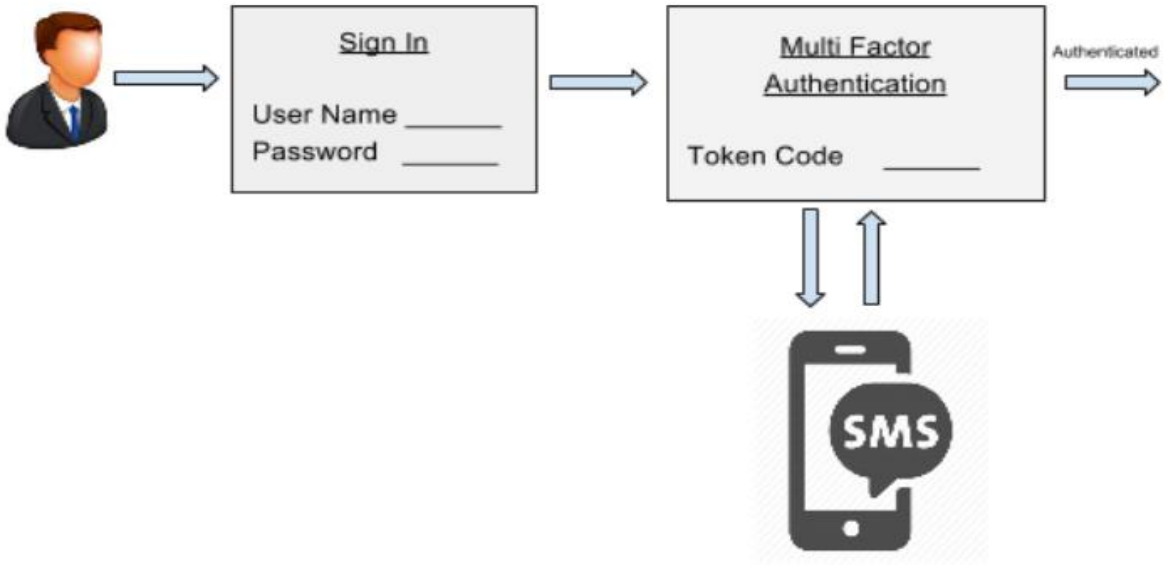


Figure 1

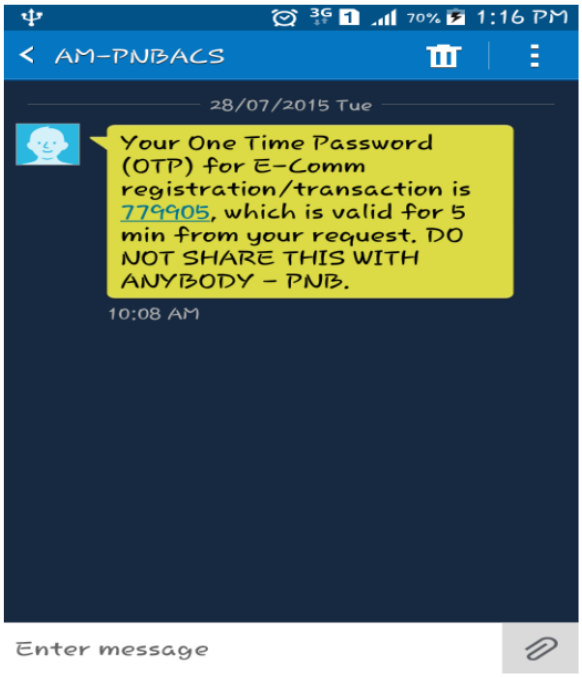


Figure 2

- **Smart phone for Authentication**

Authentication plot depends on OTP utilizing individual enrolled gadgets interface for entering OTP. On confirmation of OTP through enlisted gadget interface, coordinate communication begins among customer and server.

Authentication plot in for monetary exchanges, which is utilizing near field communication (NFC), biometric and PIN. For making exchanges, PDA application is utilized to enter sum and afterward recipient's subtle elements are gotten through NFC. Face picture of sender will be taken and on fruitful check, 4 digits PIN are utilized for authentication to finish exchange. Client burden is confinement of this plan.

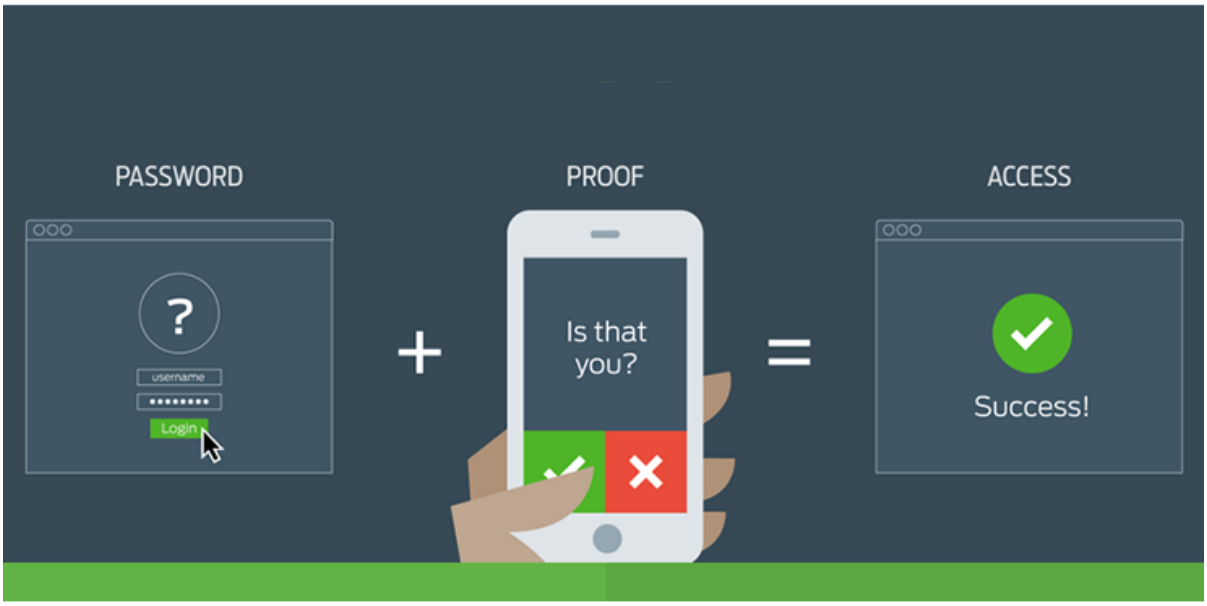


Figure 3

- **Risk based authentication**

Risk based authentication ascertains risk score related with login data. Risk is determined for gadget explicit data or social and area-based data. Access director sends content to gadget utilizing web server and assembles gadget data and ascertains risk score. On the off chance that risk is beneath the limit esteem, client is permitted to get to cloud benefits generally staggered authentication is done. On the off chance that risk score is higher, QR-code is exchanged to client through client through email or SMS benefit. Pseudo irregular number generator calculation produces dynamic QR code with arbitrariness. Impediment of risk-based authentication plot is client's association profile must be identified for figuring risk score and inappropriate location may prompt unapproved get to.

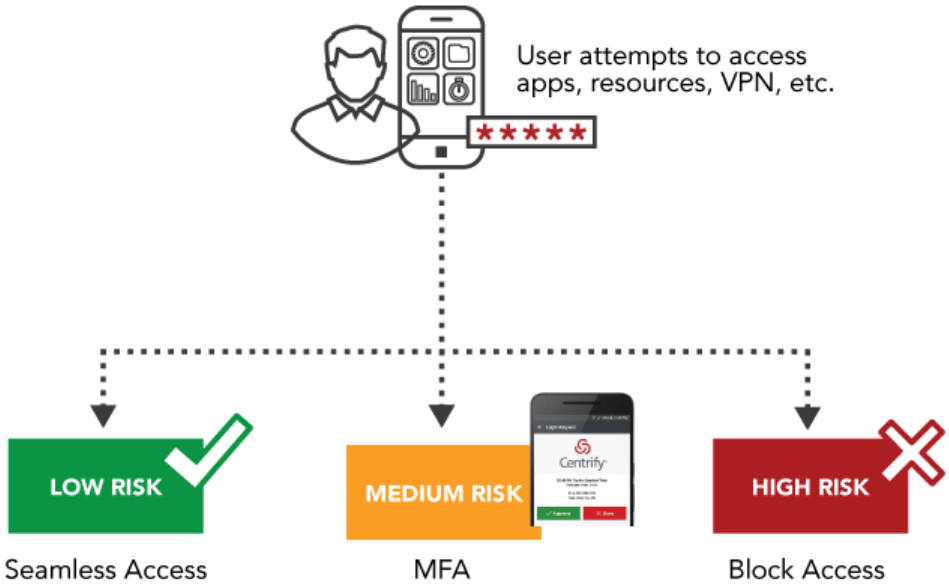


Figure 4

- **Biometric authentication**

Biometric authentication might be founded on physical, mental or social attributes. Biometric scanner is required for filtering individual's physical biometric attributes. Biometric qualities incorporate unique mark, voice acknowledgment, iris sweep, or face acknowledgment. Enlisted cell phone can be utilized for biometric input. Authentication server installs login connection to enlisted cell phone to permit biometric check. If there should be an occurrence of enlisted versatile lost, email account is utilized as option. Login interface is sent to email account and any computing gadget with installed biometric scanner can be utilized for authentication. This plan is impervious to numerous sorts of assaults as it requires predefined cell phone for filtering biometric data.

SMS based authentication gives an extra layer to biometric for online exchanges. This plan out of band channel for sending OTP which can result is delays if there should be

an occurrence of system disappointment. It additionally includes equipment cost. Biometric check along access code introduced in where all communication is encoded with RSA calculation. Client gives biometric filter and gets get to code in email. On check client will be verified and issued approved endorsement.

Figure 5

- **Graphical Password**

Graphical password depends on choosing pictures in explicit request or framing certain examples. Graphical password is more secure than printed passwords however require more space for putting away pictures. Covering example can be utilized which decrease the risk of surfing assault yet design is statics. In this, initial step 3X3 picture network where client chooses four pictures mix while in second step 3X3 framework containing 9 hint focuses is shown. Client is required to join these focuses to attract password example to get abnormal state authentication.

Utilizing mix of username and picture-based password is likewise incredible. Alphabetic pictures are given in same request as position of characters in username. Various arrangement is produced dependent on alphabetic pictures which are utilized for authentication reason.

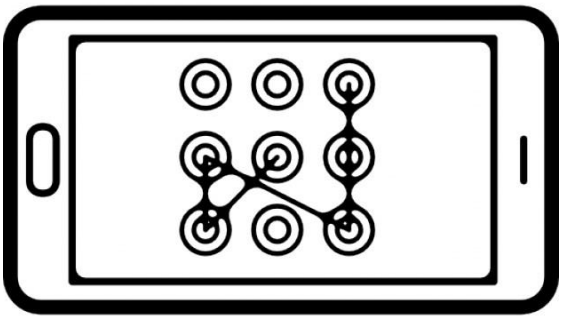


Figure 6

- **Smart card-based authentication**

Two factor authentication "2CAuth" by incorporating brilliant card and QR based authentication. Brilliant card creates irregular number and scrambles it into QR-code. Enrolled cell phone decodes QR-code by getting one stick from enlisted versatile and other from client. This unscrambled QR-code is utilized for finishing exchanges.

In "3CAuth" and incorporated brilliant card, mystery stick, biometric and cell phone-based authentication, client embed savvy card and give unique mark, at that point unscrambles QR-code utilizing his enrolled cell phone to acquire OTP. It likewise

considers timestamp for submitting QR-code. It is secure to replay, phishing and refusal of administration assault.

In encoded literary password and biometric data in shrewd card. Customer embeds brilliant card into card peruser and gives his printed password and biometric check. Cloud server matches client data with data encoded in keen card. Ownership of brilliant card is confinement of this procedure as client needs to convey it with him.

- **3D password**

3D password is blend of acknowledgment and review based characteristics. Authentication which depends on mix of printed, graphical and biometric password. This plan contains numerous choices for staggered authentication like grouping of exercises, graphical password, literary password or biometric check. Client is allowed to pick any number of blends among the accessible alternative. 3D password conspires proposed in where client performs grouping of exercises while exploring through a 3D virtual condition. 3D brisk body calculation is utilized for point determination which depends on raised body calculation. No extra equipment is required for this plan.

4D password is to reinforce 3D password with motion acknowledgment. Client perform motions for going into 3D condition. Time window is related with signals to guarantee the authenticity of client. Authentication plot dependent on 3D virtual condition are slower and require more circle space.

Figure 7

- **Sequence of activities**

Authentication scheme dependent on arrangement of exercises, where exercises incorporate menu movement, mouse action or content field action. This scheme centers around secure utilization of outsider server. Client initially enter his username and password which are send to server for check and start application program. Information from phony database is taken to stack counterfeit screen into program where client perform succession of foreordained exercises. In the event that grouping performed by client is right the first screen is stacked and coordinate communication among customer and server starts. Preferred standpoint of this scheme is that no additional equipment is required. In riddle understanding scheme proposed, in view of literary password and foreordained exercises. Client illuminate confuse in an explicit example in given time stamp. In the event that grouping matches, client get validated to utilize cloud administrations. Foreordained movement-based schemes utilize static example which can be distinguished by aggressor.

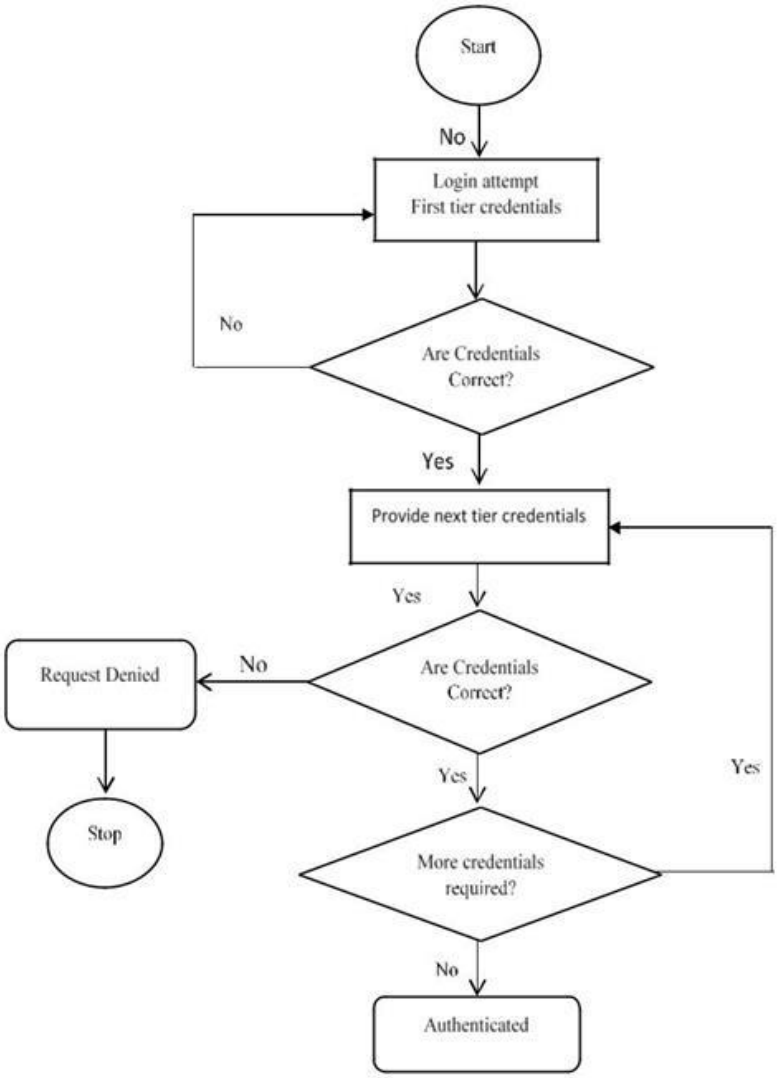
- **Multilevel authentication**

It generates and use password at multiple levels to access cloud services. Cloud administrative panel are categorized into multiple levels according administrative areas. Decision is responsible for accepting and denying logic request.

First level uses password and unique identification number whereas in second level, grid of 3X3 is displayed for graphical pattern. User selects images in sequence and then provide unique identification number to access services.

Multiple levels of organization are generated to enable strict authentication and authorization, passwords i.e.

1. Level 1(Organization level): Organizational password is required at this level for authentication. After this second level of authentication is required after the first level of authentication is successful.
2. Level2(Team level): Team password is required at this level for authentication and after which user level authentication is carried out.
3. Level3(User level): User is required to provide his password for gaining full access to resources.



Work Flow of multi-tier Authentication

Figure 8

- **Main Security Threats**

The Cisco Fog idea can be seen in a wide and coordinated way as a business visionary of many trend setting innovation advances. It might include, duplicate and influence some upgraded highlights, for example, fast examination, interoperability among

gadgets, expanded reaction time, brought together equipment the executives, low data transfer capacity utilization, productive power utilization, control instruments, and numerous others. Comparable techniques like Fog computing have now been taken to expand the ease of use and potential outcomes of Cloud stage. With the coming of such utilize, fog and comparable conditions like Edge computing, Clouds and Micro-server farms are defenseless against assaults that can influence secrecy, honesty and openness.

Cloud Security Alliance has distinguished twelve basic security issues, including different analysts. These numbers specifically influence the dissemination, sharing and request nature distributed computing. With the end goal to be ecologically neighborly like Cloud, heavyweight can likewise influence similar dangers. Our examination pursues twelve security issues to shape an efficient survey:

- Advance Persistent Threats (APT): These are cyber-attacks whose aim is to compromise a company's infrastructure with the desire to steal data and intellectual property.
- Access Control Issues (ACI): Because of poor management and any unauthorized user are able to acquire data and permissions to install software and change configurations.
- Account Hijacking (AH): In this an attack aims to hijack user accounts for malicious purpose. Phishing is a potential technique for account hijacking.
- Denial of Service (DoS): Legitimate users are prevented from using a system (data and applications) by overwhelming a system's finite resources.
- Data Breaches (DB): are when sensitive, protected or confidential data is released or stolen by an attacker.

- Data Loss (DL): It is when data is accidentally deleted from the system. This does not have to be resulting from cyber-attack and can arise through natural disaster.
- Insecure APIs (IA): Many Cloud/ Fog providers expose Application Programming Interfaces (APIs) for customer use. The security of these APIs is pivotal to the security of any implemented applications.
- System and Application Vulnerabilities (SAV): They are exploitable bugs which arises from software and configuration errors that an attacker can use to infiltrate and compromise a system.
- Malicious Insider (MI): A user with authorized access to the network and system, but has intentionally decided to act maliciously.
- Insufficient Due Diligence (IDD): It arises when an organization rushes the adoption, design and implementation of any system.
- Abuse and Nefarious Use (ANU): It arises when resources are made available for free and malicious users utilize said resources to undertake malicious activity.

    Shared Technology Issues (STI): It occurs due to sharing infrastructures, platforms or applications. Such as, underlying hardware components may not have been designed to offer strong isolation properties.

CHAPTER 2

LITERATURE SURVEY

Uymatiao, Mariano Luis T., and William Emmanuel S. Yu (2014) have taken a shot at Time-based OTP through secure passage (TOAST). They have all things considered built up a portable TOTP conspire utilizing TLS seed trade and scrambled disconnected keystroke. The principle target of this exploration is to expand after existing cryptographic benchmarks and web conventions to plan an option multifaceted validation cryptosystem for the web. It includes seed trade to a product based token through a login-ensured Transport Layer Security (TLS/SSL) burrow, encoded neighborhood stockpiling through a secret phrase secured keystroke (BC UBER) with a solid key determination work, and disconnected age of one-time passwords through the TOTP calculation. Validation happens using a mutual mystery (the seed) to confirm the rightness of the one-time secret phrase used to verify.

Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin and Jean-Pierre Seifert (2014) have chipped away at SMS-based One Time Passwords that were acquainted with counter phishing and different assaults against different web administrations like in Banking Services. Presently days, these OTPs are utilized for confirmation and approval in different applications. In any case, they are likewise inclined to exceptionally substantial assaults particularly to Smartphone Trojans. In this way, they all in all examination the security engineering of SMS OTP frameworks and study assaults. Likewise, they proposed an instrument to verify SMS OTPs against basic assaults and explicitly against Smartphone Trojans.

MichielAppelman, Yannick Scheelen (2012) have broke down on Google's 2-step confirmation login framework. In which, Google requested a confirmation code in blend with username and secret phrase. This one of a kind check code can be produced by means of three techniques for example check code can be sent by means of email or to the cell phone through voice call or an instant message. Another way is Google presents an exceptional Smartphone application that creates check codes on clients Smartphone that are legitimate just for 30 seconds of time.

Subashini K., and G. Sumithra (2014) have taken a shot at Secure multimodal portable validation utilizing one time secret key. There are a few issues with regards to security worries in these various and changing enterprises with one basic feeble connection being passwords. Most frameworks today depend on static passwords to confirm the client's character. Be that as it may, such passwords accompany significant administration security concerns. Clients will in general utilize simple to-figure passwords, utilize a similar secret phrase in various records, compose the passwords or store them on their machines, and so forth.

Himika Parmar, Nancy Nainan, and SumaiyaThaseen (2012) have by and large dissect on phishing assault and gives the need to forestall such phishing assaults. In this way dependent on this proposes not to utilize passwords and to verify a client without a content secret word. They proposed a verification administration that is picture based and dispenses with the need of content passwords. In which a client will get OTP through the texting administration accessible in web after picture confirmation. The OTP at that point can be utilized by client to get to their own records. It coordinates Image based validation and HMAC based one time secret word to accomplish abnormal state of security in verifying the client over the web.

Nitin Mujal, R. Moona (2009) portrayed a safe and savvy exchange model for budgetary administrations. Likewise with the coming of the internet business, it has turned out to be a lot simpler for the gatecrashers or assailants to sit in non-engaging area and unobtrusively siphon away the cash from the administration clients. In this manner likewise the money related administration outlets like Automated Teller Machine (ATM), Point of offer (PoS) terminal have additionally been an obvious objective. As the clients are compelled to believe an administration outlet to be credible however they can be mock and furthermore a caricature outlet can gather the record data of the clients and can utilize the equivalent to do monetary exchanges. These outlets are likewise pricey to actualize. Hence a protected and savvy model has been proposed to conquered different securities and cost related issues of money related administration models. It is practical with the end goal that money related administrations can likewise reach to the rustic populace and add to country improvement. It depends on open key foundation (PKI) design to give guarantees about both expense and security issues.

M.M. Mohammed, M. Elsadig (2013) gave a multi-layer of multi factors verification model for Online Banking Services. The security dangers of web banking have dependably involved worry for the specialist co-ops just as for the clients. Different online conditions like web banking, electronic exchanges and money related administrations have been examined to recognize the attributes and issues of existing validation strategies so as to show a client confirmation level framework model that is appropriate for various online administrations. Multifaceted Authentication has been coordinated with multi layer validation strategies so as to create a standard layered multifaceted confirmation model appropriate for various internet banking

administrations reasonable dependent on hazard evaluation criteria. The proposed model incorporates 5 levels to such an extent that each dimension contains one or mix of different validation factors, for example, information based, ownership based, or biometric based components. The standard model is contrasted with multi layering rules and it indicates improvement and satisfaction of confirmation needs.

HojinSeo, Huy Kang Kim (2011) proposed a novel way to deal with avoid e-budgetary occurrences by dissecting the info examples of portable financial clients, for example, to what extent it takes by the client to include information into a cell phone, and the ordinary finger weight levels when client contributions through a touch screen. This can help in recognizing the contrasts between the authentic client's use design and an aggressor's use design. This proposed strategy indicates high exactness and is viable in forestalling e-money related episodes.

CHAPTER 3

SYSTEM DEVELOPMENT

3.1Analysis

Multiple factors involved in Authentication Process	**Extra Hardware Required**	**Security Tiers**	**Presence of authentication control towards**	**Features**	**Limitations**
Arithmetic captcha calculation, OTP and IMEI based authentication	YES	3	Server	Resistant to many type attacks	Out of band/Hardware Cost
Requires user's personal information before sending OTP	YES	3	Server	Resistant to many type attacks	User inconvenience
Generate security token using pre-shared number, GPS, time stamp	NO	2	Client/Server	Cost effective	Clock synchronization problem
Personal device	YES	2	Client/Server	OTP must	Use of

interface for entering OTP				be entered through personal device interface	registered devices
NFC, Face Recognition and PIN	NO	2	Server	Biometric Verification through mobile front camera	Possession factor
Risk based authentication	NO	2	Server	Provide alternate way of login in case user tries to access from unregistered device	Improper detection may lead to unauthorized access
Biometric Scan using registered device	YES	2	Client/Server	Specific device for Biometric input	Hardware Cost

Biometric and SMS	YES	2	Server	Reduce risk of Biometric	Cost/Out of Band

				Photographing	channel
Biometric and Access Code	NO	3	Server	Reduce risk of Biometric Photographing	Biometric scanner cost
Graphical Pattern	NO	2	Server	Cost Effective	Static pattern
Smartcard, Biometric and QR code using registered mobile phone	NO	3	Server	Registered device for Decrypting QR-code	User inconvenience
Smartcard and Biometric scan	NO	3	Server	Multiple factors required for accessing services	Smartcard possession
3-D Password (Predetermined Activities)	NO	3	Server	Quick authentication scheme because of simplicity of scheme	Static activities and are predictable

4-D Password (3-D Password + Gesture)	NO	4	Server	Identifies the existence of human and avoids botnet automatically	Complexity and lengthy password scheme for users
Puzzle Solving	NO	2	Server	Cost effective	Static so may be predicted
Multiple Level like organizational level, team level and user level	NO	3	Server	Good for organization using Intranet	Only applicable to Intranet not to internet

3.2Design

For the design part we have taken Multilevel Authentication as the base. We will use 4D Password technique in conjunction to Graphical pattern technique but we will modify graphical pattern technique to suit our needs.The Multilevel Authentication provides a basis to divide our fog network according to the resources required.

We will divide the network into 3 tiers:

1. Tier 1: The lower most level of resources as well as the tier with least requirement for security, so we will follow the basic principle which has the Username, Password and an PIN to login.

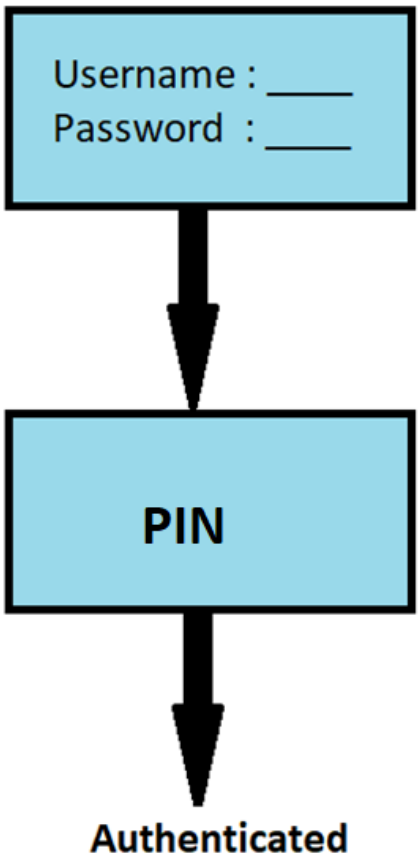


Figure 9

2. Tier 2: The middle level of resources which requires a higher level of security. It will have the basic Username, Password, PIN and an OTP to login.

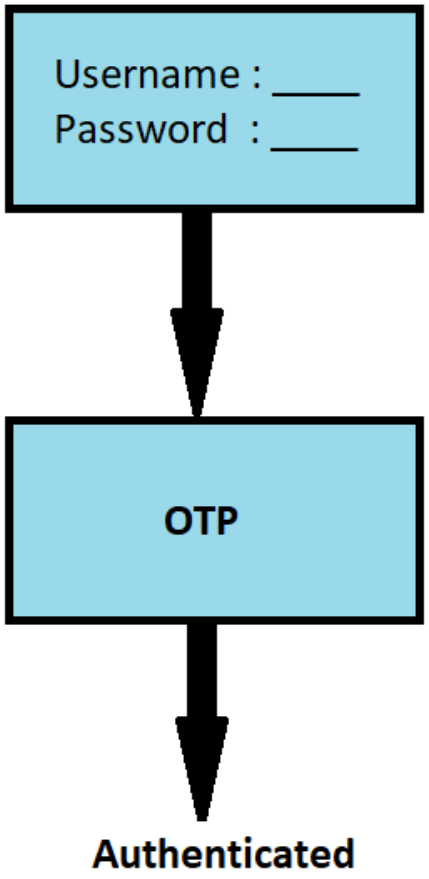


Figure 10

3. Tier 3: The level with the highest resources as well as most important data requiring highest level of security. To secure this level we use Username, Password, PIN, OTP and 4D Password scheme as well as a Graphical pattern. Each login will have a new graphical pattern which will be displayed for 1 minute on an application installed on the user's smartphone. We will also provide an alternative to the Graphical password which will consist of two random security question from a bank of 6 security questions which the user will have to fill at the time of registration.

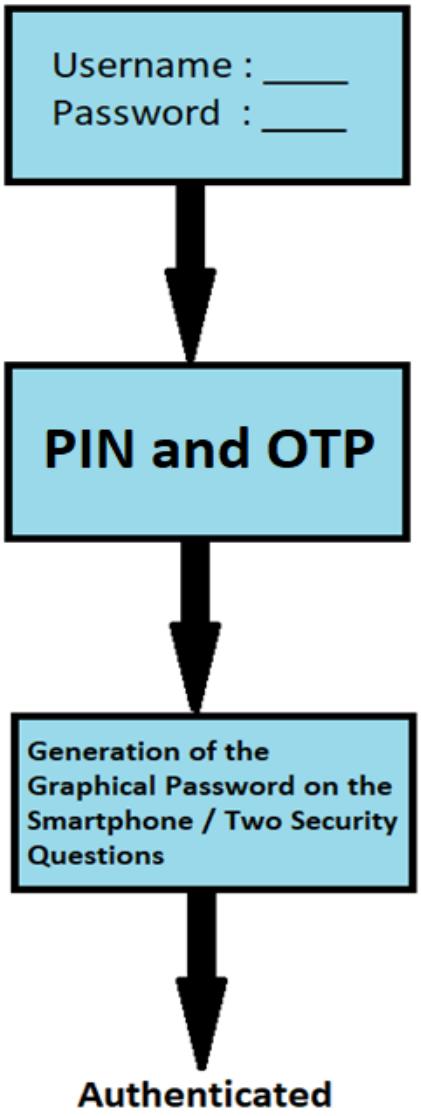


Figure 11

This level of security should be more than sufficient to meet most of the security concerns other than the lengthy process of authentication which only increases with the level of security required. The 4D Password scheme in itself is a 4th tier security scheme, adding another layer to it only increases the security.

CHAPTER 4

ALGORITHM

- **Tier 1: Username, Password and PIN**

A randomly generated PIN is provided to user whenever a new user joins and without the verification of this PIN no user can login even with Username and Password.

```
public class NewClass
{
    static char[] PIN(int len)
    {
        String numbers = "0123456789";
        Random rndm_method = new Random();
        char[] otp = new char[len];
        for (int i = 0; i <len; i++)
        {
            otp[i] =
            numbers1.charAt(rndm_method.nextInt(numbers.length()));
        }
        return otp;
    }
    public static void main(String[] args)
    {
        int length = 4;
        System.out.println(PIN (length));
```

```
        }
}
```

- **Tier2: Username, Password, Pin and OTP**

A One-Time Password (OTP) is a secret phrase or code which is substantial just for one login session or exchange on a PC framework or any computerized gadget. OTPs were acquainted just with stay away from the inadequacies that are related with static passwords. Indeed, even they are substantial for a little timeframe and they consequently terminates after the given time length. The most significant favourable position of OTPs, as opposed to static passwords, is that they are not helpless against replay assaults. It implies that a potential gate crasher or assailant who figures out how to record an OTP that was at that point utilized by a client to login into the administration won't most likely reuse it since it will be never again substantial. Additionally, OTPs are extremely hard for people to retain. Another favourable position is that a solitary OTP code can't be utilized to login on various frameworks. Numerous Techniques have been acquainted today with produce and convey these one-time passwords and the majority of them use Time-based One Time Passwords. A portion of the OTP age methods are:

In light of Time-synchronization between validating server and the customer giving the login subtleties. In Time-based One Time Password age strategy, time is a significant part in secret key calculation as the age of new secret key depends on current time as opposed to on past secret word or any mystery key. Cell phones or comparable cell phones which runs programming that is exclusive, open source or freeware is utilized to produce these occasions synchronized pass codes. A case of time synchronized passwords is Time-based One-Time Passwords (TOTP).

In light of Mathematical Algorithms in which each new One-time Passwords are produced from the past OTPs utilized. In this novel password are created from a specific mystery key or seed esteem utilizing hash work.

For the OTP part we will use TOTP or Time-based One-time Password algorithm which is an extension of HOTP or HMAC-based One-time Password algorithm. It uses the uniqueness of the current time to generate a new one-time password.

TOTP uses the HOTP algorithm, substituting the counter with a non-decreasing value based on the current time.

TOTP value(K) = HOTP value(K, C_T)

The time counter, C_T, is an integer counting the number of durations, T_X, in the difference between the current Unix time, T, and some epoch (T_0; cf. Unix epoch); the latter values all being in integer seconds.

```
public class TOTP {

 private static final int[] DIGITS_POWER
 // 0 1 2 3 4 5 6 7 8
 = { 1, 10, 100, 1000, 10000, 100000, 1000000, 10000000, 100000000 };

 private TOTP() {
 }

 private static byte[] hmacSha(String crypto, byte[] keyBytes, byte[] text) {
```

```
  try {
   Mac hmac;
hmac = Mac.getInstance(crypto);
SecretKeySpecmacKey = new SecretKeySpec(keyBytes, "RAW");
hmac.init(macKey);
   return hmac.doFinal(text);
  } catch (GeneralSecurityExceptiongse) {
   throw new UndeclaredThrowableException(gse);
  }
 }

public static int generateTOTP(byte[] key, long time, int digits, String crypto) {

byte[] msg = ByteBuffer.allocate(8).putLong(time).array();
byte[] hash = hmacSha(crypto, key, msg);

  // put selected bytes into result int
  int offset = hash[hash.length - 1] & 0xf;

  int binary = ((hash[offset] & 0x7f) << 24) | ((hash[offset + 1] & 0xff) << 16) |
((hash[offset + 2] & 0xff) << 8) | (hash[offset + 3] & 0xff);

  int otp = binary % DIGITS_POWER [digits];
  return otp;
 }
}
```

- **Tier3: Username, Password, Pin, OTP and Graphical Pattern**

The Image-based Authentication (IBA) depends on Recognition Technique. It is practically like content one-time passwords as in this likewise the client is given a mutual mystery as a proof of his/her character. In any case, content-based OTPs utilize alphanumeric characters to speak to the mystery and IBA utilizes visual data. At the point when the client enrols out of the blue on the site, they are required to choose a lot of pictures that are anything but difficult to recall, for example, regular landscape, vehicles and so forth. Each time a client login into the site or administration, they are given a framework of pictures arbitrarily produced. At that point, the client can recognize the pictures recently chosen by them. The client is validated by accurately distinguishing the secret key pictures. The classification of pictures is put away by the verification framework on Image Identification Set (IIS). At the point when a client login, the IIS for that client is just recovered and is being utilized to verify that specific client. The human is progressively adroit in recovering or reviewing a recently observed picture instead of a recently observed content. In an examination directed at University of California at Berkeley, Image-based validation (IBA) frameworks have been found easier to use than generally utilized content secret word frameworks.

Principle favourable position of IBA is that it is progressively secure and requires less memory. Picture based confirmation additionally keeps from social designing assaults, as it is simpler to verbally portray the content secret word to the aggressor but instead if there should be an occurrence of picture passwords no one can uncover for all intents and purposes depict the passwords. Albeit graphical passwords might be shared by means of taking photographs, taking screen shots or even through illustration however it clearly requires additional time than content passwords.

Likewise, thought of utilizing pictures as one-time passwords makes it hard for the aggressor to meddle utilizing Brute Force assault. Be that as it may, this likewise encourages to information control and translation to a more noteworthy degree than the alphanumeric characters do. This multifaceted nature, nonetheless, makes IBA harder to execute and send, requiring situations with expanded computational power and graphical capacities. This avoids it to be utilized by the majority of the administrations of sites as a result of multifaceted nature.

Hotspots: The real downside if there should be an occurrence of security in Image-based verification is Hotspots. Hotspots are the particular zones in a picture that have a higher likelihood of being chosen by a large portion of the clients as a piece of their passwords. In the event that any assailant can precisely anticipate the hotspots in that picture, a word reference of pictures can be assembled premise on these hotspots. Along these lines, hotspots are intended to be risky in Image-based validation.

To avoid this downside IBA is replaced with Image as an OTP with these pictures containing Graphical Pattern required to login thus eliminating the need to save apicture in memory and can avoid stealing of pattern as a new picture is generated and used every time a person logins his/her id.

CHAPTER 5

CONCLUSION

In this article by investigating the advantages and disadvantages of different accessible login authentication plans, initially we gave an account of officially accessible multi-step authentication instruments, how they work, how they are utilized, where and why.

Ordinarily utilized authentication strategies are: OTP, Smartphone based, Risk based, Biometric, Graphical Password, Smartcard based and Multilevel Authentication.

Pretty much every sort of authentication framework talked about above is broadly utilized today to give security to the clients. Once Passwords are an effective procedure to create passwords arbitrarily each time for client. OTP keep clients from replay or listening in assaults. These passwords are substantial just for given time allotment consequently there is no danger that they can be reused by an interloper to login to client account as they are invalid after one-time use. Once Passwords can be produced either on the web or disconnected yet disconnected age is better as it can likewise be created regardless of whether there is no system network and it additionally keeps from the man in the center assault.

Future Scope

Different OTP producing component are furnished with greater security step by step. New thoughts might be acquainted with expel any residual purposes of weakness as yet staying in frameworks being used today. There is a need to additionally solidify existing authentication plans with the end goal that they are simpler to utilize however progressively complex to break..

REFERENCE

- Awais Manzoor, Abdul Wahid, Munam Ali Shah, Adnan Akhunzada, Faisal Fayyaz Qureshi "Secure Login Using Multi-Tier Authentication Schemes in Fog Computing"
- I. Al Rassan and H. Al Shaher, "Securing Mobile Cloud Using Finger Print Authentication," *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 6, pp. 41– 53, 2013.
- M. M. Mohammed and M. Elsadig, "A Multi-layer of Multi Factors Authentication Model for Online Banking Services," in *International Conference on Computing, Electrical And Electronic Engineering*, 2013, pp. 220–224.
- D. R. Thorat and S. S. Sonawane, "Risk Based Multilevel and Multifactor Authentication using Device Registration and Dynamic QR code based OTP Generation," *Int. J. Adv. Res. Comput. Commun. Eng. Vol. 3, Issue 10, Oct. 2014*, vol. 3, no. 10, pp. 8312–8316, 2014.
- K. Virgile and H. Yu, "Securing Cloud Emails Using Two Factor Authentication Based on Password / Apps in Cloud Computing," *Int. J. Secur. Its Appl.*, vol. 9, no. 3, pp. 121–130, 2015.