TRACING THE IP ADDRESS AND DETAILS OF UNDEFINED PARTICIPANTS WHILE ACCADEMIC SESSIONS

PHASE 1 REPORT

Submitted by

Aswathy Suresh (RCAS2021MCS219)

in partial fulfillment for the award of the degree of

MASTER OF SCIENCE
SPECIALIZATION IN
INFORMATION SECURITY AND CYBER FORENSICS

DEPARTMENT OF COMPUTER SCIENCE

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021 (INDIA)

DECEMBER-2022

RATHINAM COLLEGE OF ARTS AND SCIENCE
(AUTONOMOUS)
COIMBATORE - 641021

BONAFIDE CERTIFICATE

This is to certify that the Phase1 entitled **TRACING THE IP ADDRESS AND DETAILS OF UNDEFINED PARTICIPANTS WHILE ACCADEMIC SESSIONS** submitted by **Aswathy Suresh,** for the award of the Degree of Master in Computer Science specialization in **"INFORMATION SECURITY AND CYBER FORENSICS"** is a bonafide record of the work carried out by her under my guidance and supervision at Rathinam College of Arts and Science, Coimbatore.

Ms.Kavitha V Kakade,M.E
Supervisor

Mr.P.Sivaprakash,MTech (Ph.D)
Mentor

Submitted for the University Examination held on 02.12.2022

INTERNAL EXAMINER

EXTERNAL EXAMINER

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021

DECLARATION

I, **Aswathy Suresh**, hereby declare that this Phase 1 entitled **"TRACING THE IP ADDRESS AND DETAILS OF UNDEFINED PARTICIPANTS WHILE ACCADEMIC SESSIONS",** is the record of the original work done by me under the guidance of **Ms.Kavitha V Kakade M.E**, Faculty Rathinam college of arts and science, Coimbatore. To the best of my knowledge this work has not formed the basis for the award of any degree or a similar award to any candidate in any University.

Place: Coimbatore **Signature of the Student:**

Date: 02.12.2022 **Aswathy Suresh**

COUNTERSIGNED

Ms.Kavitha V Kakade M.E

Supervisor

Contents

Acknowledgement

On successful completion for project look back to thank who made in possible. First and foremost, thank **"THE ALMIGHTY"** for this blessing on me without which i could have not successfully my project.I am extremely grateful to **Dr.Madan.A. Sendhil, M.S., Ph.D.,** Chairman, Rathinam Group of Institutions, Coimbatore and **Dr. R.Manickam MCA., M.Phil., Ph.D.,** Secretary, Rathinam Group of Institutions, Coimbatore for giving me opportunity to study in this college.I am extremely grateful to **Dr.R.Muralidharan, M.Sc., M.Phil., M.C.A., Ph.D.,** Principal Rathinam College of Arts and Science(Autonomous), Coimbatore.Extend deep sense of valuation to **Mr.A.Uthiramoorthy, M.C.A., M.Phil., (Ph.D),** Rathinam College of Arts and Science (Autonomous) who has permitted to undergo the project.

Unequally I thank **Mr.P.Sivaprakash, MTech., (Ph.D).,** Mentor and **Dr.Mohamed Mallick, M.E., Ph.D.,** Project Coordinator, and all the Faculty members of the Department - iNurture Education Solution pvt ltd for their constructive suggestions, advice during the course of study.I convey special thanks, to the supervisor **Ms.Kavitha V Kakade,M.E.,** who offered their inestimable support, guidance, valuable suggestion, motivations, helps given for the completion of the project.

I dedicated sincere respect to my parents for their moral motivation in completing the project.

List of Figures

List of Abbreviations

OTP	One Time Password
SMB	Server Message Block
SIP	Session Initiation Protocol
WebRTC	Web Real-Time Communication
URL	Uniform Resource Locator
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
UDP	User Datagram Protocol
API	Application programming interface
RTOC	Real-Time Operating Centre

Abstract

Identity management includes frameworks, processes, and activities that enable authentication and authorization of legitimate individuals to access E-Learning platforms.During the COVID pandemic situation, education has changed drastically with the distinctive rise of digital learning. The links for the instructional classes/webinars are shared by some students with miscreants who login to the session using the same hyperlink by means of using the identification or name of other autherised participants. Mischievous students create indiscipline, confusion, and use foul, abusive language to disturb the whole meeting.This paper will solve the problem by establishing a second authentication mechanism that uses an OTP to confirm the user and blocking the IP addresses of undefined participants in an academic session. It will be easy for the host to block such intruders before entering the session, and it should not be displayed on the chat box or displayed during the session. This paper can give 75% accuracy.

Chapter 1

Introduction

Worldwide school closures are the result of COVID-19. Around the world more than 1.2 billion students are not in school.As a result, education has changed drastically, with the distinctive rise of e-learning, whereby teaching is undertaken remotely and on digital platforms.Then the students shifted from the classroom to an online class. Online learning has become the new normal. With the rise of remote learning, many virtual learning tools have emerged, including Google Meet, DingTalk, Google Classroom, Zoom, and Webex, among others. The lockdowns, the closure of schools and distance learning had a deep impact on the mental health of students. The frustrations among the students affected their activities as well as behavior, which disturbed the whole class and the decorum of the session The links for the instructional classes/webinars are shared by some students with miscreants who login to the session using the same hyperlink by means of using the identification or names of other autherised participants. After logging into the meeting, miscreants and mischievous students create indicipline, confusion, and use foul and abusive language to disturb the whole meeting.Messages, which are usually disturbing and offensive, need to be blocked in such a way that they

are not shown in the chat box or displayed during the session.

The goal of this paper is to identify the intruders and miscreants, and they should not be able to use the ID's and names of the autherised participants or students.It should be easy for the host to block such intruders, which does not happen usually. By identifying the disruptive attendees in the session, this study will assist in reducing disruptions during academic sessions. Using a manually configured open source video conferencing tool (Jitsi). It aids in the identification of authenticated users by determining the IP address of an incoming request. Establishing a second authentication mechanism that uses an OTP to confirm the user.In Jitsi server,which generates the OTP at the time of login and sends it to the student email address. As a result, we can easily identify and block the undefined participants before entering into the session.

1.1 Objective of the project

During the pandemic situation 993 universities, 39931 colleges, and 10725 stand-alone institutions were left closed, according to records kept by the MHRD Government of India. Since the middle of March 2020, over 32 crore students have been subjected to various restrictions and a statewide lockdown (Jena,2020). Many universities have launched online learning as an alternative to face-to-face learning in the midst of this lockdown to provide unbroken learning possibilities. Academicians' only remaining choice for conducting academic work is online learning, which is in conformity with the COVID-19 safety precautions. Many professional educational institutions, such as those that train teachers, have begun dispensing their courses in ways that emphasise

the importance of both theory and practise.

The Students are misbehaving in;

1.Cheating(sending the session link to the miscreants)

2.Unautherised participants misbehaving in sessions,Recording the videos of the session for making fun of them

3.Students turn off their camera,put themselves on mute, and then they use their phone to play games or text buddies.

4.After attendance is collected, just leave the room, knowing that their teacher is having trouble using the technology and won't notice or know what to do.

5.Changing participants' name

The main target of this project is to enhance the security of online sessions with an extra authentication method by sending an OTP to the student's registerd email id and block the undefined users before entering into the session.

1.2 Scope of the Project

In the modern era, having access to knowledge is essential for career success. The days when learning and education were only available at colleges and universities are long past. Learning is accessible to everyone in the digital era. For those who encounter difficulties obtaining a traditional college degree, e-learning is a blessing. Globally, online education has altered the knowledge economy.

According to recent World Economic Forum research, India has more than 2,000,000

students enrolled in online courses, surpassing the United States in terms of online course enrollments. Reputable colleges provide excellent, accredited online courses, sending top-notch professors and teachers to teach the students.Indian students have a great deal of enthusiasm for the idea of online learning. They have the chance to demonstrate their abilities and skills in a sophisticated, dynamic setting. A high-quality education is now accessible to everyone thanks to online courses and certification programmes.

The main goal of education is to advance one's status. Online courses and certification programmes have made it possible for the general public to receive affordable education while also saving time, effort, and money. A wide variety of courses that are tailored to the student's main interests are offered through accredited online courses, creating a favourable environment for future progress. Employers erroneously believe that traditional brick-and-mortar college graduates are preferred. On the other hand, the high skill levels of students who have completed online courses and certification programmes from highly regarded educational institutions are being acknowledged by corporate organisations in India.

When face-to-face communication is not available, educators and students frequently use videoconferencing as a learning tool to promote effective communication between students and teachers or students and their peers. Today's higher education institutions use a variety of platforms or systems for videoconferencing.Few students distribute the links to the academic sessions and webinars to miscreants, who then use the same link to check in to the meeting using the IDs and names of other identified attendees. After

logging in, miscreants cause chaos, confusion, and filthy language to permeate the entire class. This paper will help to reduce the disturbances during the academic sessions by identifying the unwanted participants in the session.Through the configuration of open source video conferencing tool(Jitsi). which identifies the IP address of an incoming request and helps to identify the authenticated users. Setting up an extra authentication method that verifies the user with an OTP.

.

1.3 Existing System

Webex:

You can remotely meet with other individuals through a Webex meeting without leaving your house or place of business. A computer with Internet connectivity and a dedicated phone line are needed for Webex meetings. You can view the presenter's computer screen by connecting to the meeting over the Internet.Products from Cisco Webex offer features including file sharing, group messaging, and online meetings. The suite is regarded as a top unified communications platform for collaboration and is designed for both large-group meetings for enterprise-wide deployments and small-group collaboration for SMBs. This service is more expensive than some of the rival online collaboration tools. Some people complain that the user interface and system menu are not very friendly. If you connect using a platform other than Webex, you can have audio problems. It is difficult to switch from legacy Webex platforms to this cloud-based version.

Google meet:

Google Meet provides enterprise-grade video conferencing and meetings to let teams of all sizes connect and collaborate. The platform touts many business users and provides tools like whiteboarding, breakout rooms, polling, and more to increase meeting engagement. Screen sharing is a useful platform offered by Google Meet, but it only allows the sharing of one screen at a time. As the meeting creator, there are instances when you are unable to add more attendees and are informed that your membership has been exceeded. You can connect only 100 participants at a time for virtual meetings.There have been several complaints registered by Google Meet users who experienced freezing of the browser while sharing the screen.

Zoom:

Zoom is a cloud-based video conferencing service that you may use to conduct live discussions while digitally meeting with others. Zoom also allows you to record those sessions for later viewing.Early in 2020, worries about Zoom's security and issues with unauthorised visitors known as Zoombombers were voiced. Insecure Zoom meetings were being sought out by some people, who would then enter them before "bombing" the call with pornographic material, graphic videos, and other inappropriate material.

Chapter 2

Literature Survey

Recent studies in the reviewed literature have attempted to ascertain if computer-mediated education, such as e-learning or hybrid learning, is superior to conventional face-to-face teaching in terms of, for instance, learning outcome and student satisfaction. Researchers, educators, and those who make decisions about education are all interested in learning which format produces the best outcomes for students and educational institutions.

2.1 Approaches to Online Learning and Concept Drift for User Identification in Computer Security[1]

Terran Lane and Carla E. Brodley

In this study, the approaches for classifying temporal sequences of nominal data as being similar to or distinct from previously observed sequence data when the underlying notion is subject to drift are examined. The function of anomaly detection in computer security is where this issue originates (Kumar, 2020). The objective of this area is

to profile the behaviours of a computer user (the "valid" or "normal" user) in order to identify odd events by comparing the current input stream to the profile. In this work, we are faced with a variety of difficult problems, such as learning from discrete, non-metric time sequence data, learning from examples from just one class, learning online, and learning while concepts are drifting.

2.2 Security Exercises for the Online Classroom with DETER[2]

Peter A. H. Peterson, Peter L. Reiher

A new online security education focusing on the application of computer security was developed in response to UCLA's establishment of an online master's degree programme in computer science in 2007. Online learning faces an unusual difficulty because the coursework must be just as good and educationally valuable as "offline" homework while still being simple to use and access without much face-to-face interaction. To develop live security exercises with realistic scenarios, customise DETER Linux disc images. A number of the widely used and well-liked open-source tools, some of which are standard tools for security work, were used to develop every component of the labs. Regular talks with the professor during office hours, progress reports, and presentations are frequently part of the quarter-long research project in UCLA's traditional graduate-level CS courses. The online master's programme uses prerecorded lectures and is therefore appealing to students who work full time and may not have suitable schedules, even though some of this contact could take place over video chat. A group of physical devices

and programmable routers that can be dynamically configured and accessible over the Internet make up the DETER testbed. A thorough lab handbook with background details, interesting scenarios, references to internet resources, and summaries of the pertinent software tools is provided with this setup.

2.3 Motivators and concerns for real-time online classes: focused on the security and privacy issues[3]

Sang So Kim

Discovering how to increase student involvement is essential because education is moving more and more online as a result of the COVID-19 pandemic; hence, in-depth research into the factors that encourage and hinder student participation is required. This study especially focused on security and privacy concerns as the main problems that may be limiting student involvement given the characteristics of an online learning environment. This study provided the results of the structural model test demonstrating that perceived utility and peer behaviour significantly influence real-time online class participation intentions based on the data collected from 296 students studying at Y University, South Korea.This study also found the harmful impacts of privacy and security concerns on perceived participation ease, which in turn affects RTOC participation intention via perceived utility and peer behavior. This study's methodology will offer analytical implications that support student engagement and active learning since technology-enabled contactless activities, including online education, have become the

new norm.

2.4 Data Security and Privacy in Times of Pandemic[4]

Luis Fernandes

The world-wide effects of the coronavirus were so terrible that the World Health Organization was forced to declare a pandemic condition. This occurred on March 11, 2020, and it compelled governments and other institutions to impose curfews and shut down cities and nations. Organizations and the general public had to adapt to these safeguards, which exposed some openings for hackers to exploit. Since the advent of the internet and its incorporation into virtually every aspect of our lives, including business and leisure, data security and privacy have become increasingly important.Because this virus is new and the information about it was not accurate, there was a lot of false information being spread online, and as a result, organisations were not prepared to make these modifications and were compelled to do them rapidly. Data security refers to defending our digital information against those, referred to as hackers, who gain access to it without authorization.This article will also outline certain requirements and potential measures from a number of firms that offer crucial services in order to protect our privacy and the security of our data. This article will also look at a few examples from those eras and discuss what could be learned from them.

Chapter 3

Methodology

3.1 Opensource Video Conferencing Tool(Jitsi)

For the web platform, Windows, Linux, macOS, iOS, and Android, Jitsi is a set of free and open-source multiplatform voice (VoIP), video conferencing, and instant messaging applications. The Jitsi Desktop marked the start of the Jitsi project (previously known as SIP Communicator). The project team's attention has since switched to the Jitsi Videobridge in order to support web-based multi-party video calling due to the rise of WebRTC. Later, the team launched Jitsi Meet, a comprehensive video conferencing tool with clients for the web, Android, and iOS. In addition, Jitsi runs meet.jitsi, a free community-hosted version of Jitsi Meet.With the help of simple-to-use and highly secure technologies, you may arrange video conferences with Jitsi Meet, a free video collaboration platform. You can send invitees a link to a meeting on the website using Jitsi Meet. Group video, live chat, screen sharing, streaming, and other features are provided.

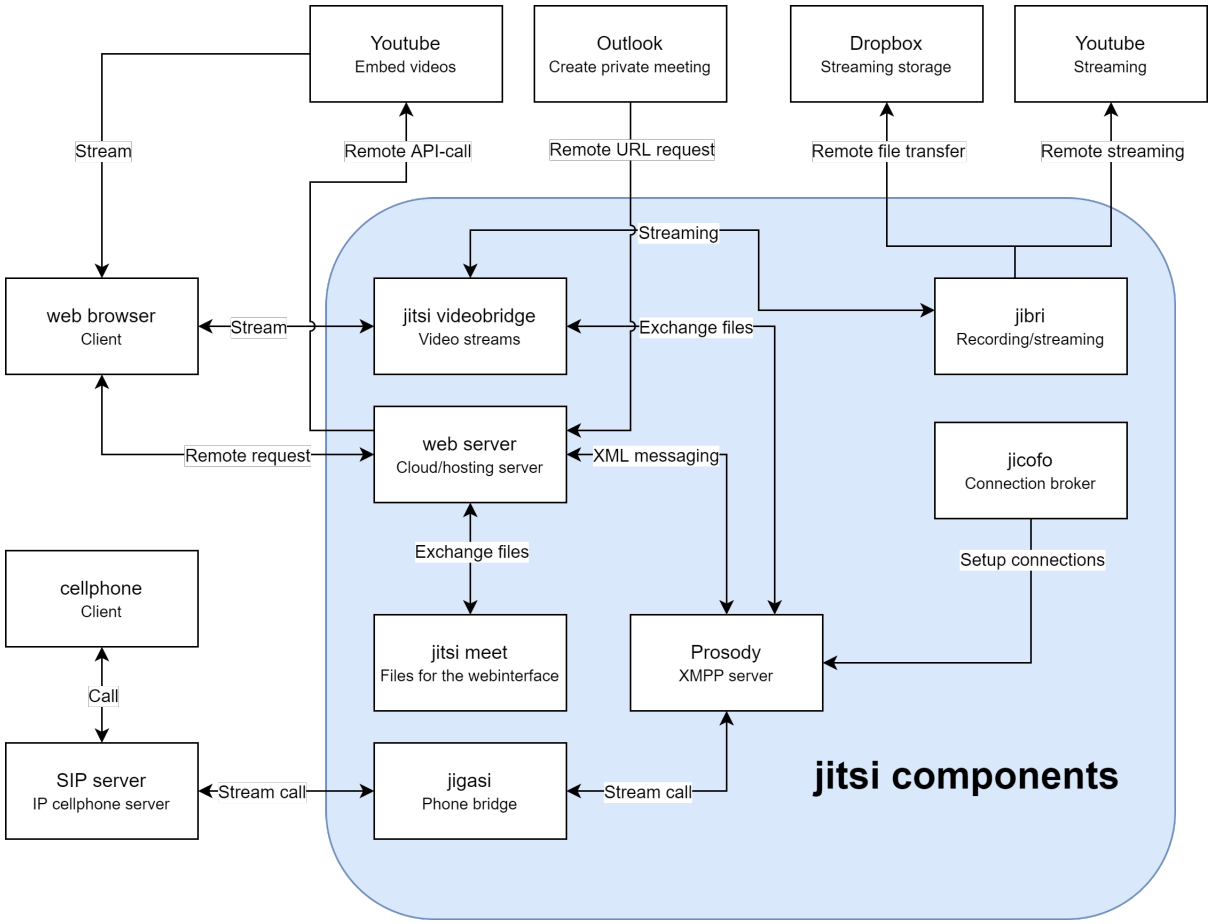

Figure 3.1: Jitsi Components

3.2 Video conferencing server

Flexible, easy-to-use, and secure video conferences Jitsi Meet, an open-source (Apache) WebRTC JavaScript application that functions as a Zoom substitute, uses Jitsi Videobridge to deliver high-definition, secure, and scalable video conferencing.Without installing anything else on your computer, the Jitsi Meet client operates within your browser.It makes collaboration extremely effective. The user's desktop or specific windows can be streamed. With Etherpad, it also offers collaborative document editing.

FEATURES

Jitsi Meet is a completely secure option. Share presentations, your desktop, and more. Using a straightforward, personalised URL, invite folks to a conference. Together, edit documents with Etherpad. For each meeting, choose engaging meeting URLs. While you are in a video conference, you can talk while exchanging messages and emojis. Opus and HD audio. No need for creating a profile. with default encryption (and advanced security settings). Access the current speaker automatically, or click any attendee to view their video. Add a password to a room's lock. A live conference stream on YouTube. Statistics on participant talk time. Play a YouTube video for everyone present. Option for just audio. Dialling in over the phone to a conference (if Jitsi is setup). Dial-out to a participating phone number (if Jitsi is setup).

3.3 System Design

.

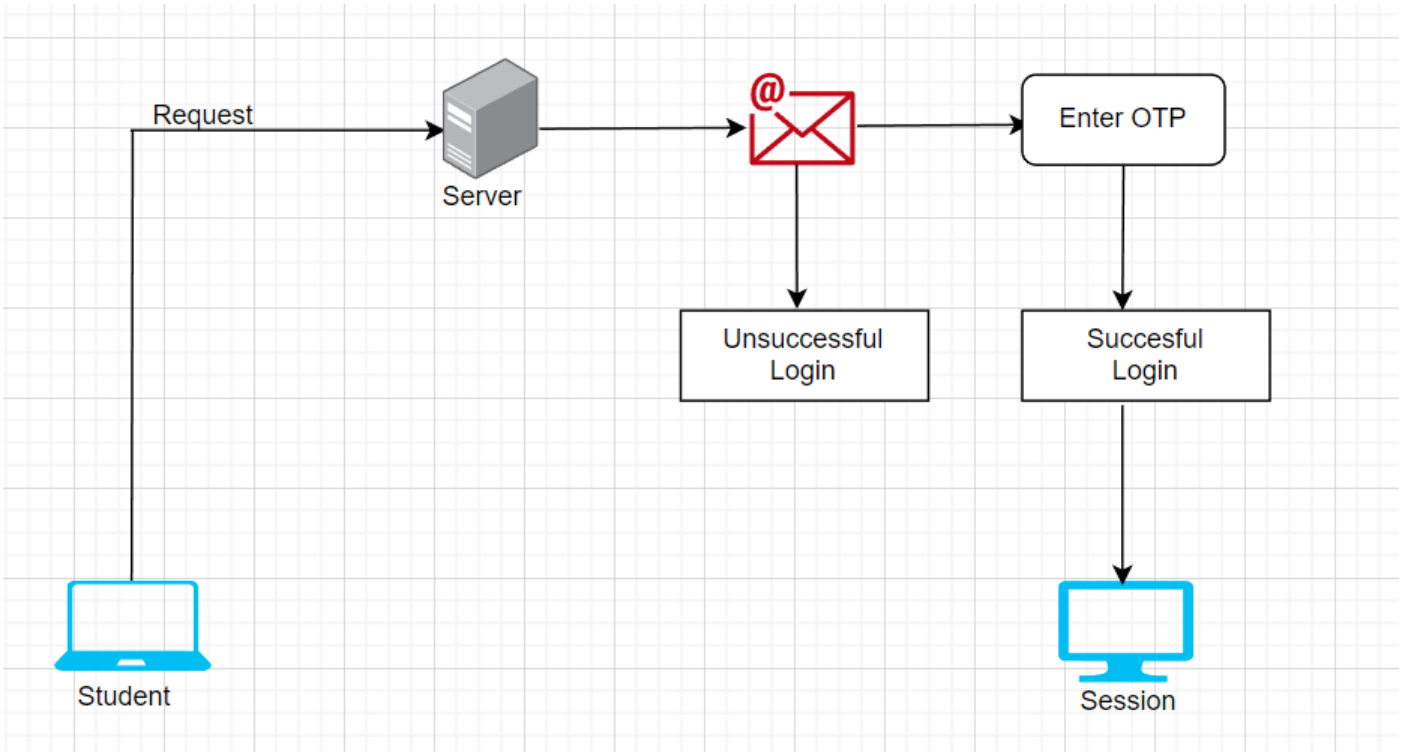

Figure 3.2: System Design

Chapter 4

Experimental Setup

4.1 Configuring the video conferencing tool into server

Step 1: Prepare a server machine

-Server resource

1GB RAM, 2GHz CPU, 25 GB DISK, 10GbE Net.

-Operating system

Ubuntu 16.04 Xenial Xerus LTS recommended or other GNU/LINUX

-Access

root SSH or User SSH with sudo

user@server$sudosu – root@server$

-Firewall

80 TCP(HTTPS)

443 TCP(HTTPS)

10000-20000 UDP

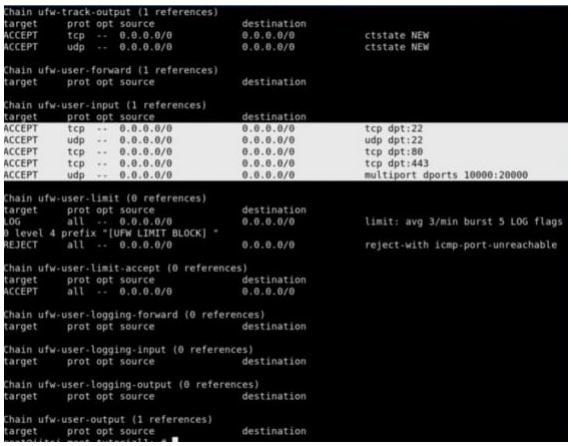

Figure 4.1: Firewall Setup

-DNS Name

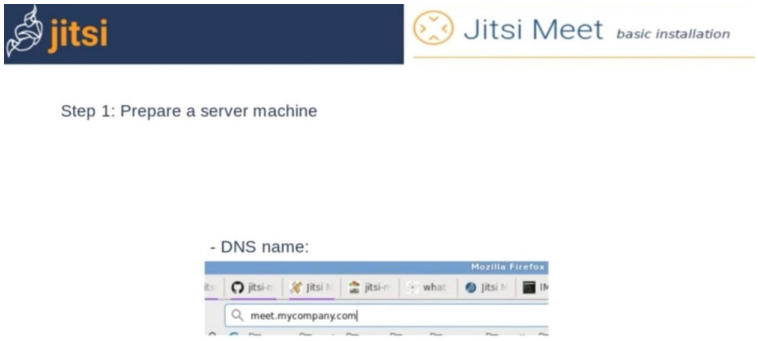

Figure 4.2: Domain Name

Step 2: Add a Jitsi repository

- Add the Jitsi Key from:

Wget https://download.jitsi.org/jitsi-key.gpg.key

gpg jitsi-key.gpg.key

gpg - -search-keys dev@jitsi.org

gpg - - list-sigs dev@jitsi.org

gpg -recv-keys. . .

apt-key add jitsi-key.gpg.key

- Add the Jitsi repository

echo ‘deb https://download.jitsi.org stable/’¿ /etc/apt/sources.list.d/jitsi-stable.list

Step 3: SSL Certificate

-already available certificate

/etc/ssl/dnsname.crt - - certificate file

/etc/ssl/dnsname.key - -key file

certificate from LetsEncrypt self-signed certificate

Step 4: Install the packages

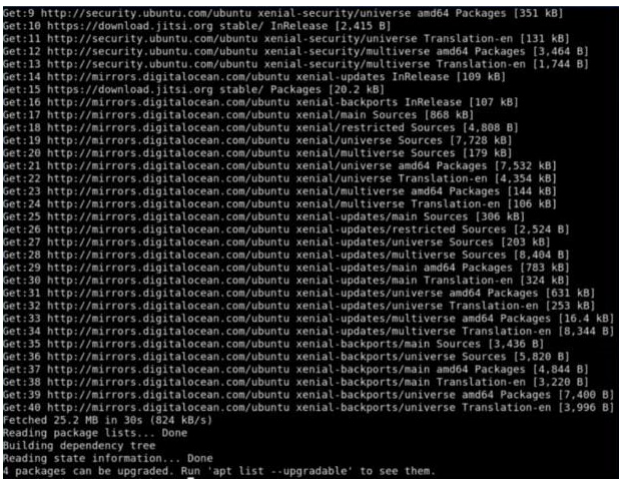

Figure 4.3: Package Installation

Step 5: Check and start

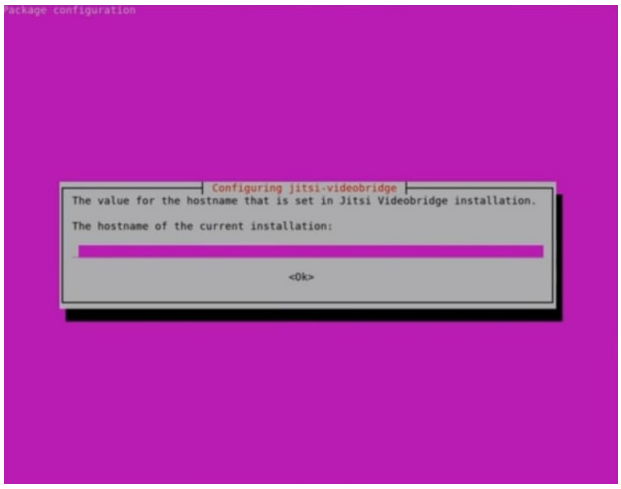

Figure 4.4: Configuring Videobridge

4.2 E-mail OTP Verification

When a system notices that a user's login attempt is suspect, it will send a one-time password to the user's email. Using the Google Recaptcha API is a useful approach to spotting fraudulent requests.The OTP is a random String with a length of 8 characters (and it is supposed to be unique among all users). Within five minutes, the OTP will be expires. The user should enter the OTP, which can be received in his email, within this specified timeframe.

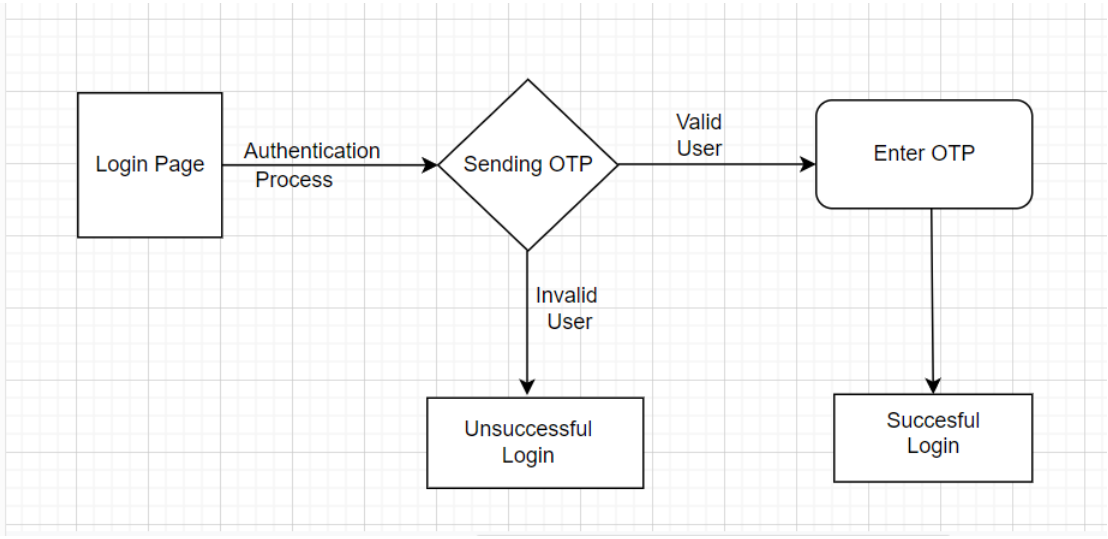

Figure 4.5: OTP Verification

Step 1:Authentication Header Creation

String customerKey = "<YOUR_CUSTOMER_KEY>";

String apiKey = "<YOUR_API_KEY>";

String currentTimeInMillis =

String.valueOf(System.currentTimeMillis());

String stringToHash = customerKey + currentTimeInMillis + apiKey;

String hashValue = new

Sha512Hash(stringToHash).toHex().toLowerCase();

HttpPost postRequest = new HttpPost("");

postRequest.setHeader("Customer-Key", customerKey);

postRequest.setHeader("Timestamp", currentTimeInMillis);

postRequest.setHeader("Authorization", hashValue)

Step 2: OTP Generation

{

”customerKey”:”<OUR_CUSTOMER_KEY>”,

”phone”:”<PHONE_NUMBER_TO_SEND_OTP_TO>”

”email”:”<EMAIL_TO_SEND_OTP_TO>” /

”authType”:”SMS or EMAIL”

”Name”:”CUSTOM-OTP-VERIFICATION”,

}

JSON Response generated via Generate Rest API.

{

”txId: ”<UNIQUE_TRANSACTION_ID>”,

”authType: ”Email”,

”responseType: ”CHALLENGE”,

”emailDelivery”: {

”contact”: ”<EMAIL_ADDRESS_OTP_WAS_SENT_TO>,

”sendStatus”: ”SUCCESS”,

”sendTime”: ”<TIMESTAMP>”

}

”status”: ”SUCCESS”,

”message”: ”Successfully generated.”

}

Step 3: Validating OTP

{

"txId": "fc727646-7c91-11e5-883e-0e2fb063e0f9",

"token": "123456"

}

JSON Response generated via Generate Rest API.

{

txId: "<UNIQUE$_{T}RANSACTION_{I}D¿$"

responseType: "VALIDATE"

status: "SUCCESS"

message: "Successfully Validated"

}

Chapter 5

Results and Discussions

The objective of the study is to build a framework that identifies the undefined participants in an academic session and blocks the miscreants who login to the session with the id and name of the identified participants. This system identifies and blocks the undefined participants in academic sessions by an OTP verification.By configuring an additional verification method on the server, the host can conduct the meeting in a secure and private room, and the admin can create a secure password for that particular session.Predicting that the system will provide 75% accuracy.

Chapter 6

Conclusion

Digital learning is growing in popularity after the pandemic situation. E-learning platforms offer a way forward for the education system. Online education One of the main issues that the e-learning platform faces is that unauthorised people log in to the class and cause chaos, indiscipline, and use abusive language in order to disrupt the entire meeting. This paper reduced the problems faced during online sessions. By identifying the disruptive attendees in the session and reducing the disruptions during academic sessions using a manually configured open source video conferencing tool (Jitsi). It identified authenticated users by determining the IP address of an incoming request and establishing a second authentication mechanism that uses an OTP to confirm the user. Jitsi server, which generates the OTP at the time of login and sends it to the student's email address. As a result, we easily identified and blocked the undefined participants before they entered the session.

6.1 Future Works

TThis paper's future work should aim to improve the security of the user's personal data. Sometimes students will get into the class, and they will play games, watch movies, and chitchat. It should not allow any unwanted applications during the class session, and that can be monitored by the admin so that the admin can monitor the student's activities. The host can't monitor the student's activity. By implementing a technique that computes the switching count as well as the duration of usage by other applications, the host can calculate the amount of time the students have left in that session, and anti-cheating measures can be implemented to avoid cheating.

References

1. Terran Lane and Carla E. Brodley.1998"Approaches to Online Learning and Concept Drift for User Identification in Computer Security." School of Electrical and Computer Engineering,Purdue University,West Lafayette, IN 47907-1285 terran,brodley @ ecn.purdue.edu

2. Peter A. H. Peterson., Peter L. Reiher.2010 "Security Exercises for the Online Classroom with DETER." CSET 2010: 3rd Workshop on Cyber Security Experimentation and Test.

3. Sang Soo Kim.2021. "Motivators and concerns for real-time online classes: focused on the security and privacy issues." https://doi.org/10.1080/10494820.2020.1863232

4. Luis Fernandes.2021"Data Security and Privacy in Times of Pandemic." Lusofona University, Porto-Portugal. a21805177@mso365.ulp.pt

5. Dooyong Jeon.,Byungchul.2019."BlackEye: automatic IP blacklisting using machine learning from security logs." doi: https://doi.org/10.1007/s11276-019-02201-5

6. Gigi Varghese.2020."Effectiveness of Virtual Learning with Security." http://www.bayancollegeijm

7. Dr.Shahid Minhas.,Tasaddaq Hussain.,Abdul Ghani.,KIRAN Sajid.2021."Exploring Students Online Learning: A Study of ZOOM Application." https://doi:10.35378/gujs.691705

8. Zuheir N Khilaaf.,Soheli Salha.2021. "The Unanticipated Educational Challenges of Developing Countries in Covid-19.https://doi.org/10.30476/ijvlms.2020.86119.1034

9. Elma Afsar.,Munam Ali Shah., Muhammad Owais.2021"Cyberbullying In online classes: The Case Of COVID-19." https://digital. library.theiet.org/content/conferences/cp786

10. Linh Dich., Heidi A. McKee., James E. Porter.2013."Ethical Issues in Online Course Design: Negotiating Identity, Privacy, and Ownership." https://journals.uic.edu/ojs/index.

11. Tam Trinh.2020."Zoom Privacy and Security Settings - Avoid sharing meeting links on social media or public Avoid using Personal Meetings ID (PMI) to host public events."CID: 20.500.12592/nm127g

12. Sunny Shrestha.,David Thomas.,Sanchari Das.2022."SecureLD: Secure And Accessible Learning for Students with Disabilities." https://doi.org/10.1177/1071181322661157

13. Vida Vilic.2021."Cyber Security and Privacy Protection During Coronavirus Pandemic." https://doi.org/10.15308/Sinteza-2021-158-164

14. Ceren ÇUBUKÇ.,Cemal AKTÜRK.2020 "The Rise of Distance Education during Covid-19 Pandemic and the Related Data Threats: A Study about Zoom." 127 - 144, 01.10.2020