BLOCKING THE UNDEFINED PARTICIPANTS WHILE ACADEMIC SESSIONS

A Thesis

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)

MAY-2023

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021

BONAFIDE CERTIFICATE

This is to certify that the Phase1 entitled **BLOCKING THE UNDEFINED PARTICIPANTS WHILE ACADEMIC 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 09.05.2023

INTERNAL EXAMINER

EXTERNAL EXAMINER

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021

DECLARATION

I, **Aswathy Suresh**, hereby declare that this Thesis Report entitled **”BLOCKING THE UNDEFINED PARTICIPANTS WHILE ACADEMIC 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: 09.05.2023 **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.S.Balasubramanian, M.Sc.,Ph.D,(Swiss),PDF(Swiss/USA)** 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, such as video conferencing, pre-recorded lectures, online discussions, and digital assessments. Many schools and universities have also adopted learning management systems (LMS) to organise and manage their digital learning materials.

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 authorised 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 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, Ding Talk, Google Classroom, Zoom, and Webex, among others. The lock downs, 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 authorised participants. After logging into the meeting, miscreants and mischievous students create indiscipline, 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 authorised 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 secure 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.Un-authorised 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 registered 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 white boarding, 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 Zoom bombers 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. The survey draws upon a variety of sources, including academic journals, conference proceedings, and other relevant publications, to provide a comprehensive overview of the current state of knowledge in this field.

The survey begins by highlighting the growing trend of online learning and the increasing use of virtual classrooms. It emphasizes the importance of ensuring that only authorized individuals have access to academic sessions, as unauthorized access can disrupt the learning process and pose a security risk. The survey then discusses the various methods that have been proposed to address this issue, including password-based authentication, bio-metric authentication, and two-factor authentication. The literature survey also explores the limitations of these methods and the challenges associated with their implementation. For example, password-based authentication is vulnerable to brute-force attacks and can be compromised if users choose weak passwords. Bio-metric authentication, on the other hand, can be difficult to implement and may require specialized hardware. Two-factor authentication, although more secure than password-based authentication, can be inconvenient for users and may require additional resources to implement.

The survey then highlights the recent developments in the field of access control and authentication, including the use of machine learning algorithms and artificial intelligence to improve security and reduce the risk of unauthorized access. It also discusses the various types of bio-metric authentication techniques, such as fingerprint recognition, facial recognition, and voice recognition, and their applications in online learning and virtual classrooms.Finally, the literature survey presents several case studies of successful implementations of access control and authentication techniques in various online learning platforms and virtual classrooms. These case studies provide evidence of the effectiveness of the proposed methods and demonstrate the importance of implementing robust security measures to protect the privacy and security of participants in academic sessions.

Overall, the literature survey provides a comprehensive overview of the current state of knowledge in the field of access control and authentication in the context of academic sessions. It highlights the importance of implementing effective security measures and presents a range of methods that can be used to address the issue of unauthorized access. The findings of the literature survey serve as a foundation for the proposed extra authentication method presented in the research paper, which aims to improve the security of academic sessions and enhance the overall learning experience for participants.

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 test bed. 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 contact less 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 Open source Video Conferencing Tool(Jitsi)

For the web platform, Windows, Linux, mac OS, iOS, and Android, Jitsi is a set of free and open-source multi platform 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 Video bridge 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.

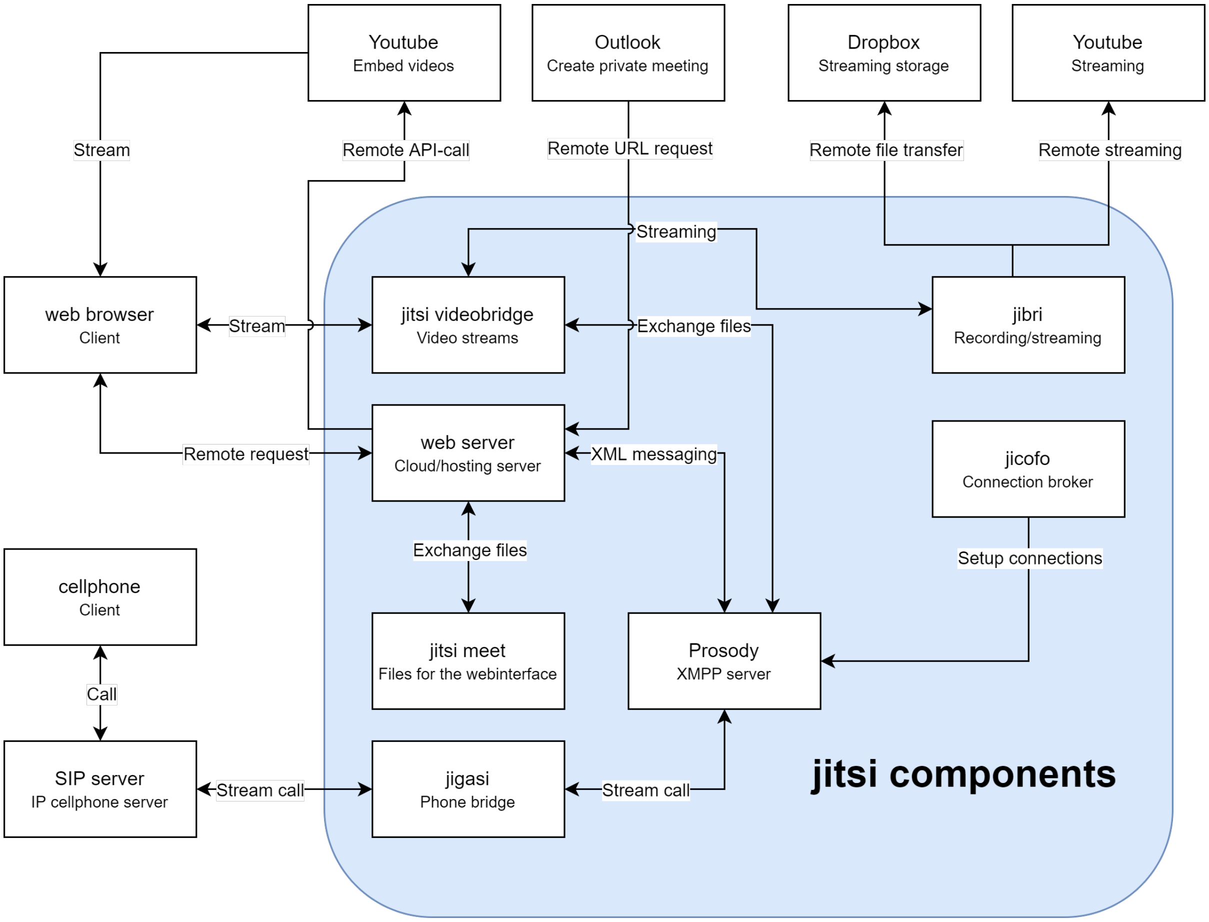


Figure 3.1: Jitsi Components

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 Video bridge 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 Ether pad, 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 Ether pad. 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

.

User Interface: The user interface of the app will be designed to provide a seamless and user-friendly experience for participants. The UI will include options to sign up or log in, create or join sessions, and input OTP verification.

Authentication and Authorization: The app will use authentication and authorization methods to ensure that only authorized users can access the academic sessions. The app will verify user credentials using email and password, and then send an OTP verification code to the user's registered mobile number.

OTP Verification: Upon receiving the OTP code, the participant will be required to input it to join the academic session. The OTP code will be sent to the participant's registered mobile number only, and will expire after a set duration to ensure security.

Session Creation and Joining: The app will provide the option for session creation by the host, who can invite participants to join the session by sharing the session link along with the OTP code. Only participants who have registered for the session and verified their OTP will be able to join the session.

Session Management: The app will provide features to manage the academic sessions, such as starting, pausing, and ending the session. The host will have administrative control over the session, and can mute or unmute participants, remove participants, or control access to the session.The host can add password for each session.

Data Privacy and Security: The app will ensure the privacy and security of the data shared during the academic sessions. The data will be encrypted using advanced encryption methods, and the app will comply with industry-standard data privacy regulations.

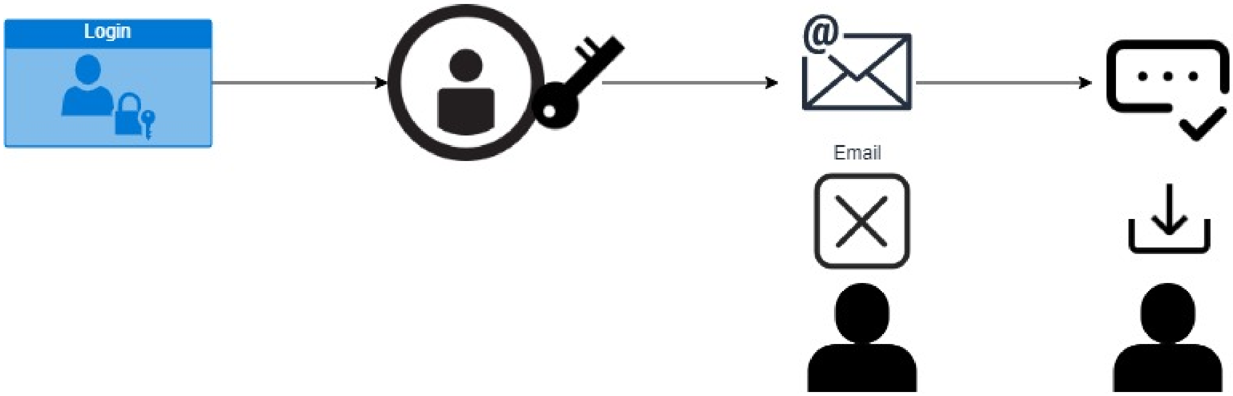


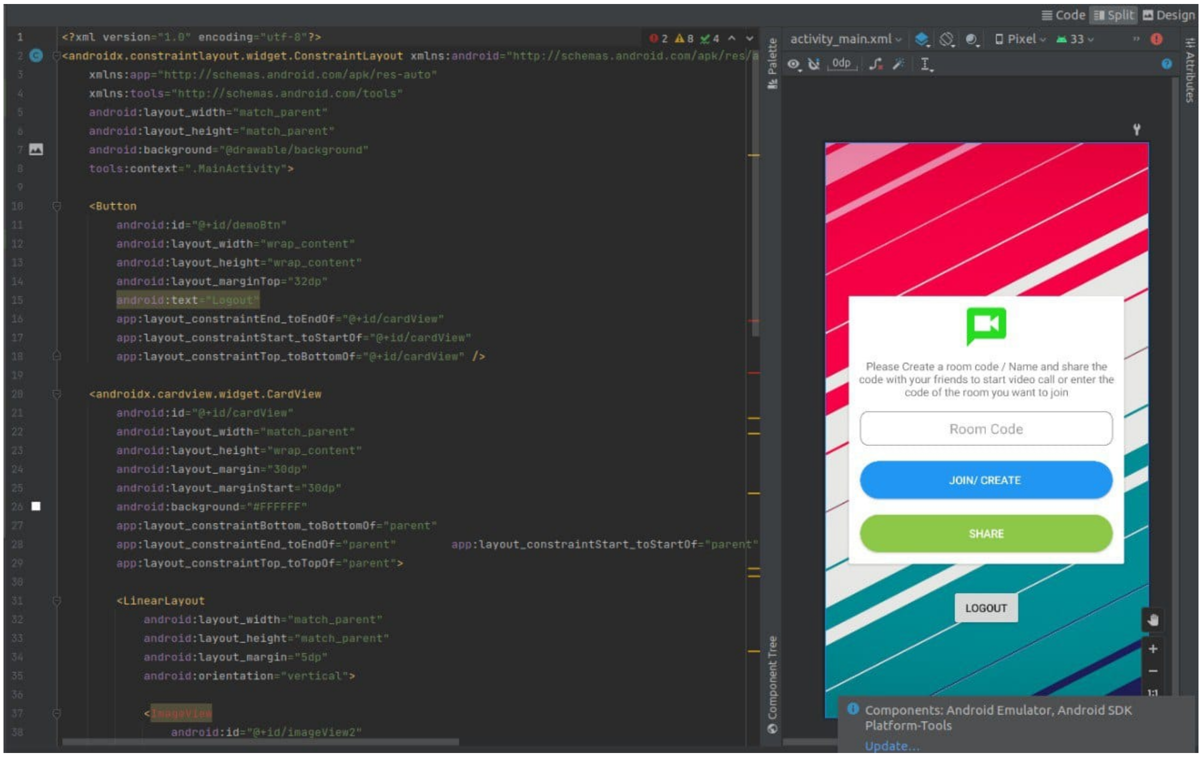
Figure 3.2: System Design

Chapter 4

Experimental Setup

4.1 Configuring the video conferencing framework

Step 1: Prepare the machine



```xml
<?xml version="1.0" encoding="utf-8"?>
<androidx.constraintlayout.widget.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/a
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:background="@drawable/background"
    tools:context=".MainActivity">

    <Button
        android:id="@+id/demoBtn"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_marginTop="32dp"
        android:text="Logout"
        app:layout_constraintEnd_toEndOf="@+id/cardView"
        app:layout_constraintStart_toStartOf="@+id/cardView"
        app:layout_constraintTop_toBottomOf="@+id/cardView" />

    <androidx.cardview.widget.CardView
        android:id="@+id/cardView"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:layout_margin="30dp"
        android:layout_marginStart="30dp"
        android:background="#FFFFFF"
        app:layout_constraintBottom_toBottomOf="parent"
        app:layout_constraintEnd_toEndOf="parent"        app:layout_constraintStart_toStartOf="parent"
        app:layout_constraintTop_toTopOf="parent">

        <LinearLayout
            android:layout_width="match_parent"
            android:layout_height="match_parent"
            android:layout_margin="5dp"
            android:orientation="vertical">

            <ImageView
                android:id="@+id/imageView2"
```

Please Create a room code / Name and share the code with your friends to start video call or enter the code of the room you want to join

Components: Android Emulator, Android SDK Platform-Tools

Figure 4.1: Video Conferencing Framework

Login Activity

User registration: Users typically need to register for an account with the video conferencing tool. During registration, users provide their personal details such as name, email address, and password. The login activity coding part involve securely storing this information in a database.

Authentication: When a user tries to log in, the tool needs to verify their identity. This is usually done through authentication protocols such as OAuth or Open ID Connect. The login activity part would involve implementing these protocols to ensure that users are authenticated securely.

Password protection: To protect user accounts, passwords need to be stored securely.The login activity part would involve implementing password and to ensure that user passwords are not exposed to unauthorized parties.

Session management: Once a user logs in, the tool needs to create a session for that user. This session allows the user to access the tool's features without having to log in repeatedly. The login activity coding part would involve implementing session management techniques such as cookies and tokens to ensure that user sessions are secure and expire after a certain amount of time.

Main Activity

Creating and managing a meeting: The tool needs to provide a way for users to create and manage a meeting. This includes inviting participants and managing their access to the meeting. The main activity part would involve implementing these features, as well as ensuring that meetings are secure and private.

Video and audio streaming: During a video conference call, the tool needs to stream audio and video data between participants. The main activity part would involve implementing real-time audio and video streaming using technologies such as WebRTC, as well as managing the quality and bandwidth of the streams to ensure a smooth user experience.

Screen sharing: Participants may need to share their screens during a video conference call to present slides, documents, or other content. The main activity part would involve implementing screen sharing features that allow participants to share their screens securely and efficiently.

Chat and messaging: Participants may need to communicate with each other during a video conference call using text-based chat or messaging. The main activity part would involve implementing these features, as well as ensuring that messages are private and secure.

Sign up Activity

Collecting user information: Collect user information such as name, email address, and password. The sign up activity part would involve implementing a user registration field that collects this information securely.

Validating user information: Ensure that the user information entered during registration is valid and meets certain criteria. This includes checking that the email address is valid and unique, and that the password meets certain strength requirements. The sign up activity part would involve implementing validation rules to ensure that user information is valid and meets the tool's requirements.

Storing user information: Store user information securely in a database. The sign up activity part would involve implementing a database schema to store user information and encrypting sensitive user data such as passwords.

Sending confirmation emails: Send a confirmation OTP email to the user to verify their email address and the user. The sign up activity part involve implementing an email system that sends confirmation emails securely and efficiently.

splash Activity

Designing the splash screen: The tool needs to design a visually appealing and informative splash screen that is consistent with the app's branding and provides useful information to the user. This may include the app logo, loading animation, and brief description of the app.

Implementing the splash screen layout: The splash activity part would involve implementing the layout of the splash screen using XML layout files. This includes specifying the position, size, and appearance of the various elements on the screen.

Loading app resources: The tool needs to load any required app resources during the splash screen loading process. This may include loading images, fonts, or other media files that are required by the app.

Implementing splash screen timing: The tool needs to determine the length of time that the splash screen is displayed. The splash activity coding part would involve implementing a timer or delay that controls when the splash screen is dismissed and the main app screen is displayed.

Optimizing splash screen performance: The tool needs to optimize the performance of the splash screen to ensure that it loads quickly and smoothly. This may include minimizing the size of the splash screen image, using a simple loading animation, and avoiding any unnecessary loading of resources during the splash screen display.

4.2 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 Re captcha 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 time frame.

One-Time Password (OTP) verification is a security measure,In video conferencing these app which verify the identity of users and prevent unauthorized access.

User initiates login: The user initiates the login process by entering their email address and password.

OTP request: Once the user has entered their login credentials, the video conferencing app will send an OTP request to the user's registered email address.

OTP generation: The video conferencing app generates a unique OTP code for the user. T

OTP delivery: The OTP code is delivered to the user's registered phone number or email address via SMS or email.

User enters OTP code: The user enters the OTP code they received into the video conferencing app.

OTP verification: The video conferencing app verifies the OTP code entered by the user. If the OTP code matches the code generated by the app, the user is granted access to the video conferencing app.

Time-based OTP: In some cases, the video conferencing app may use time-based OTPs.The OTP code will expire after a short time period.

Multi-factor authentication: To further enhance security, some video conferencing apps may use multi-factor authentication. This involves using a combination of two or more factors to verify a user's identity, such as a password and a fingerprint scan or facial recognition.

Overall, OTP verification is an effective way to prevent unauthorized access to the online sessions .By requiring users to enter a unique code generated by the app, so that we can ensure that only authorized users are able to access sensitive video calls and meetings.

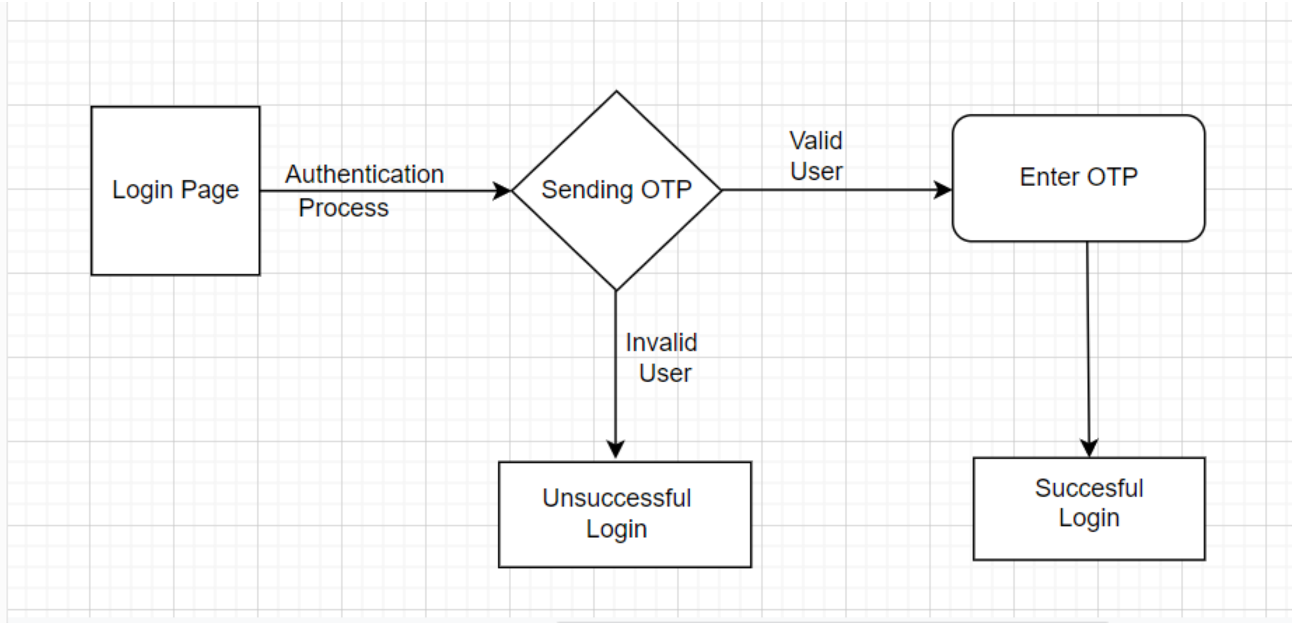


Figure 4.2: OTP Verification

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”

}

send Verification Code(): This method is responsible for sending a verification code to the user’s phone number. It uses the Phone Authentication Provider class to generate a verification code and sends it to the provided phone number. It also sets up a listener to handle the verification process. If the verification is successful, it automatically calls the sign In With Phone Authentication Credential() method to authenticate the user.

sign In With Phone Authentication Credential(): This method is responsible for authenticating the user with the provided phone number verification code. It uses the Fire base Authentication class to authenticate the user with the provided Phone Authentication Credential object. It sets up a listener to handle the authentication process. If the authentication is successful, the user is signed in.

verify Verification Code(): This method is responsible for verifying the verification code entered by the user. It creates a Phone Authentication Credential object with the verification code and verification ID and passes it to the sign In With Phone Authentication Credential() method.

show OTP Dialog(): This method creates a UI dialog for the user to enter the OTP code received on their phone. It creates an Alert Dialog object and adds an Edit Text field for the user to enter the OTP code. It also sets up two buttons - "Verify" and "Cancel". When the user clicks the "Verify" button, it calls the verify Verification Code() method with the entered OTP code.

on Login Clicked(): This method is called when the user clicks on the login button. It first retrieves the user's phone number from the Phone Number Edit Text field. If the phone number is not empty, it calls the send Verification Code() method to send a verification code to the user's phone number and then calls the show OTP Dialog() method to show the OTP verification dialog to the user

Chapter 5

Results and Discussions

The increasing reliance on online learning platforms has highlighted the need for effective security measures to protect the integrity of academic sessions. 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, you can monitor the number of participants who are able to successfully enter the room with a valid OTP, compared to the number of participants who are unable to enter the room due to invalid OTPs. OTP generation and sending success rate: Tracks the number of OTPs generated and sent successfully, compared to the number of OTPs that failed to be generated or sent. OTP validation success rate: Track the number of OTPs that were successfully validated, compared to the number of OTPs that were invalid. User experience: We can ask participants to provide feedback on the OTP verification process, and measure their satisfaction with the process. By monitoring these metrics, we can evaluate the effectiveness of your OTP implementation and make improvements as needed. Additionally, we can ensure that the OTP verification process is secure, reliable, and user-friendly. 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.The system will provide 75% accuracy.

Chapter 6

Deployment Process

6.1 Overview of the process

The objective of the experiment is to build a framework that identifies undefined participants in an academic session and blocks miscreants who login to the session with the id and name of the identified participants.The framework is designed using JavaScript. With the id and name of the identified participants, you can monitor the number of participants who are able to successfully enter the room with a valid OTP, compared to the number of participants who are unable to enter the room due to invalid OTPs. The system and techniques described in this disclosure relate to an authentication system that allows a user to authenticate through a user's account with OTP.

Creating a video conferencing framework using java script and we need to setup the settings based on our requirements.In splash activity which create a visually attractive and educational splash screen that complies with to the branding of the app and gives the user important information. This could include the programme's icon, loading animation, and short app description.Using XML layout files, the splash activity would implement the splash screen layout. This entails describing the layout, scale, and visual appeal of the various screen elements.During the splash screen loading phase, the tool must load any necessary app resources. For example, the programme could need to load photos, fonts, or other media files.The length of time the splash screen is visible must be determined by the utility. Implementing a timer or delay that regulates when the splash screen is closed and the main app screen is shown is part of the coding for the splash activity. The splash screen's performance must be optimised by the tool to guarantee a rapid and seamless loading process. This can entail reducing the splash screen image's size, employing a straightforward loading animation, and eliminating any pointless resource loading while the splash screen is being displayed.

Then the framework obtain user data from the user, such as name, email, and password. Implementing a user registration field that securely captures this information is part of the sign up activity.Make sure the user information you submit during registration is accurate and satisfies specific requirements. This involves making sure the email address is accurate and distinct, as well as that the password satisfies specific standards for strength. Implementing validation rules to make sure that user information is accurate and complies with the tool's requirements would be part of the sign up activity.Maintain user data in a database securely. Implementing a database schema to hold user information and encrypting sensitive user data, such as passwords, are both part of the sign-up activity. Send the user a confirmation OTP email to confirm their email address. Implementing an email system that sends confirmation emails safely and effectively is required for the sign up activity.

Typically, users have to create an account with the video conferencing software. Users enter personal information during registration, including their name, email address, and password. The login activity component entails safe database storage of this data.The application needs to confirm a user's identity when they attempt to log in. Authentication mechanisms like OAuth or OpenID Connect are typically used for this. Implementing these protocols would be necessary for the login activity phase to make sure that users are safely authenticated.Passwords must be properly saved in order to safeguard user accounts.Implementing a password is necessary for the login activity phase in order to protect user passwords from being revealed to unauthorised persons.The tool has to initiate a session for each user after they log in. The user can access the tool's functionality during this session without needing to log in again and again. Implementing session management strategies, such as cookies and tokens, to make sure that user sessions are secure and end after a set length of time would be part of the login activity code.

Users need to be able to create and manage sessions using the tool. This entails extending invitations and controlling attendees' access to the gathering. Implementing these features and making sure meetings are private and secure would be the key activity. The tool must stream audio and video data between participants during a video conference call. Implementing real-time audio and video streaming using tools like WebRTC would be the primary effort, along with controlling the streams' quality and bandwidth to provide a positive user experience. In order to display slides, documents, or other content during a video conference call, participants might need to share their screens.Implementing screen-sharing technologies that enable users to share their screens securely and effectively would be the primary activity. During a video conference call, participants might need to connect with one another using text-based chat or messaging. Implementing these features and making sure that messages are secure and private would be an essential activity.

6.2 User Interface

The app's user interface will be designed to provide participants with a seamless and user-friendly experience. The user interface will include options for signing up or logging in, creating or joining sessions, and entering OTP verification.To ensure that only authorised users can access the academic sessions, the app will use authentication and authorization methods. The app will use email and password to verify user credentials before sending an OTP verification code to the user's registered mobile number.The participant will be required to enter the OTP code after receiving it in order to join the academic session. To ensure security, the OTP code will be sent only to the participant's registered mobile number and will expire after a set period of time.

The user interface of the app will be designed to provide participants with an efficient and user-friendly experience. Options for signing up or logging in, creating or joining sessions, and entering OTP verification will be available in the user interface.The app will use authentication and authorization methods to ensure that only authorised users can access the academic sessions. The app will verify user credentials via email and password before sending an OTP verification code to the user's registered mobile number.In order to join the academic session, the participant must enter the OTP code after receiving it. To ensure security, the OTP code will be sent only to the participant's registered mobile number and will expire after a predetermined time period.The host can add different passwords for each sessions.

6.3 Results & Discussions

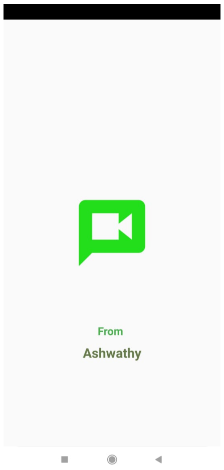


Figure 6.1: video conferencing tool

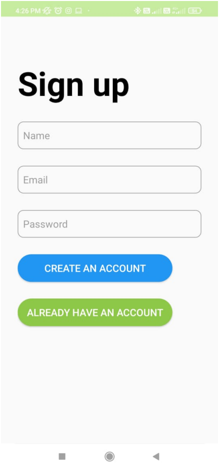
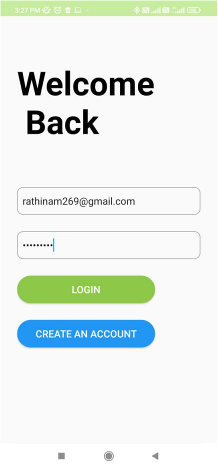


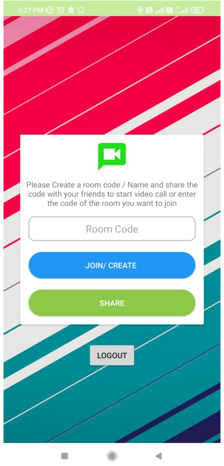
Figure 6.2: user creation



Welcome Back

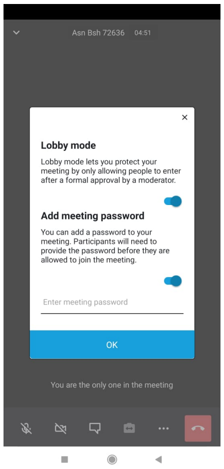
rathinam269@gmail.com

Figure 6.3: user Verification



Please Create a room code / Name and share the code with your friends to start video call or enter the code of the room you want to join

Figure 6.4: meeting creation


Asn Bsh 72636 04:51

Lobby mode

Lobby mode lets you protect your meeting by only allowing people to enter after a formal approval by a moderator.

Add meeting password

You can add a password to your meeting. Participants will need to provide the password before they are allowed to join the meeting.

Enter meeting password

OK

You are the only one in the meeting

Figure 6.5: security

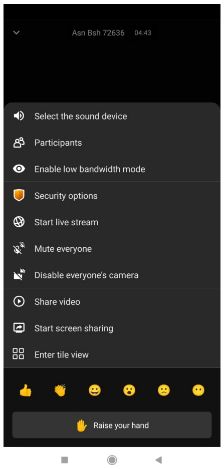


Figure 6.6: settings

Chapter 7

Conclusion

Digital learning is growing in popularity after the pandemic situation. E-learning platforms offer a way forward for the education system. With the increasing reliance on online learning platforms, ensuring the security and integrity of academic sessions has become a crucial concern for educators. In recent years, there have been several instances of unauthorized participants disrupting online academic sessions by accessing the platform using fake identities and the 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 secure video conferencing framework. It identified authenticated users and blocked the unwanted incoming request by establishing a second authentication mechanism that uses an OTP to confirm the user. 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.

7.1 Limitations

One limitation of these video conferencing framework with OTP verification is that they rely on the behavior of users. OTP verification requires users to input a unique code that is sent to their phone or email. However, if users do not follow proper security practices, such as sharing their OTP with others, then the security of the video conferencing tool can be compromised For example, if a user receives an OTP and shares it with an unauthorized person, that person could gain access to the video conference. Similarly, if a user fails to properly secure their phone or email account, an attacker could gain access to the OTP and use it to bypass the verification process. Therefore, it is important to educate users on proper security practices and monitor user behavior to ensure compliance.

7.2 Future Works

This 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

15. Nguyen Duy Khang Truong.,Tran Khanh Dang.,Cong An Nguyen.2021.”On Using Cryptographic Technologies in Privacy Protection of Online Conferencing Systems.”https://link.springer.com/chapter/10.1007/978-981-16-8062-5_8

16. M.Darshan.,S.R Raswanth.,S.Skandan.,S.Shakthi Saravanan.,Ranjit Chandramohanan., Priyanka Kumar.2022.”A Secured BlockChain Based Facial Recognition System for Two Factor Authentication Process.”

https://link.springer.com/chapter/10.1007/978-981-19-1677-9_44

17. Siqi Ma.,Runhan Feng.,Juanru Li.,SuryaNepal.,Diethelm.,Elisa Bertino.,Robert H.Deng.,Zhuo Ma.,Sanjay.Jha.2019.”An empirical study of SMS one-time password authentication in Android apps.”https://doi.org/10.1145/3359789.3359828

18. Alejo Grigera,.2015.”User Account Authentication During User Issue Resolution.”

19. Dr. Elsaeed. E. Mohamed Abd Elrazek.,Esraa.M.Ramadan.2022.”A Common Framework Based onMulti-Factor Authentication to Secure Students Log in to Educational Digital Platform.” DOI:10.21608/jetdl.2022.136241.1027

20. Essohanam Djeki.,Jules Degila.,Carlyna Bondiomboly.,Muhtar Hanif Alhassan.2022. ”Preventive Measures for Digital Learning Spaces Security Issues.”

doi:https://doi.org/10.1109/TEMSCONEUROPE54743.2022.9801945