IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

# Tracing IP Address and Details of Unidentified Participants in Webinars

**Mr. Nagaraja G[1], Prajwal P[2], Pavan Kumar PS[3], R Sai Abhiram[4], Siddesh Gundagi[5]**
Associate Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
S. J. C Institute of Technology, Chickballapur, India
nagaraj.ise@sjcit.ac.in

**Abstract:** *During pandemic the mode of sharing information with the multiple participants in physical mode is reduced, to overcome this the online mode of sharing information and discussions through webinars has been increased globally. In case of any misbehaviors from unidentified participants to stop the webinars, we need to identify the participant who is misusing the opportunity. So, we came with the idea of IP tracking. In this project we provide the option to monitor the unidentified participants and we can access the details of the participant such as IP Address. Through IP Address we can identify the participant and necessary action can be taken from the concerned authorities.*

**Keywords:** Webinars, IP Tracking, Unidentified Participant's ,Socket Programing, Reverse DNS

## I. INTRODUCTION

A webinar is a public meeting or discussion conducted over the internet. In general, the webinars are conducted in offline mode with human-to-human Interactions. But after the covid-19 pandemic the public gatherings are restriction So, the tech giants came with the idea of multiple kind of applications to communicate with the people virtually. The one of that is online meeting app which is used for virtual meeting or webinar conduction. Through the availability this kind of applications has been increased rapidly. This is the revolution in the industry of communication that took place all over the major economies. The rise of the webinars has been adopted in emergence by the Indian government with the certain regulations over it. All the activities and government meetings are started to take place in the virtual mode. Luckily with the help wide internet connectivity this isn't took long time to adopt to the people. This encouraged all the types of gatherings meetings to held online.

The webinar has been designed in such a way that it isn't make people to feel difficult over it. The webinar can host many participants at a time and the webinar has been created by the admin with his id over the platform. This this trend of webinar coming up the security, hate speech and fake id over the webinars came with surprise this again gave challenge to the tech companies. So, the companies had come with the ideas to overcome with the facing challenge. The admin has been provided with the multiple features such as blocking, restricting the person to attend the webinar by blocking him. But the same person can attend the webinar again with the different id and cause the disturbance to the webinar. So, they again came with the solution to it with blocking the IP of the specific person so that the same person who is disturbing cannot enter the webinar with that device at all. This enhanced the willingness over the public towards the webinars.

## II. LITERATURE SURVEY

[1] Title: Using Biometrics Authentication via Fingerprint Recognition
Authors: Sara Jeza Alotaibi
Abstract: Webinar is a great opportunity for modern life
Authentication of webinar takers is of prime importance so that Webinar are given by fair means. A new approach shall be proposed so as to ensure that no unauthorized individuals are permitted to give the Webinar. The fingerprint recognition is unique factor for each individual and cannot be easily modified or duplicated.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

**Methodologies:**

- Fingerprint Recognition

**Advantages:**

- It properly authenticates the participants so that no unauthorized individuals are permitted access to the webinars

**Disadvantages:**

- There is no continuous monitoring.
- It verifies the user once login in.

[2] Title: Towards Security Goals in webinars.
Authors: Kikelomo Maria Apampa; Gary Wills; David Argles
Abstract: passwords are recognized based on the key stroke that is the speed at which the keys are being operated however this doesn't hold good in all situation and it takes time to analyze the user key stroke and the technology for building it is harder but once built can be used over a long time however it sometimes does fail to recognize the original user as there might be a negligible difference in key strokes.

**Methodologies:**

- Password hardening based on keystroke dynamics

**Advantages:**

- Identity and authentication are security goals which are expected for all participants in webinar.

**Disadvantages:**

- There is no continuous monitoring.
- It is not suitable to track IP address.

[3] Title: Authentication of participants using multimodal biometric technology
Authors: Liangyuan Chen
Abstract: Biometrics, physiological and/or behavioral traits used to distinguish different individuals, have now been widely used in authentication sites because they have shown advantage over passwords and token-based verification methods. A multimodal technology is the one that has different biometric identifiers as a form of multi factor authentication.

**Methodologies:**

- Multi- biometrics

**Advantages:**

- An authentication system with multi- biometrics to support various services in user authentication

**Disadvantages:**

- There is no continuous monitoring.
- It verifies the user once login in.
- No IP tracking

[4] Title: Cryptographic Key Generation from voice
Authors: F. Monrose; M.K. Reiter; Qi Li; S. Wetzel
Abstract: We generate cryptographic keys using the voice which can be used as authentication factor for allowing user to enter webinar.

**Methodologies:**

- Cryptographic keys

**Advantages:**

- The preliminary result is very encouraging.

**Disadvantages:**

- It verifies the user once login in.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

- No IP tracking

[5] Title: Fuzzy Vault for fingerprints
Authors: Karthik Nandakumar; Anil K. Jain; Sharath Pankanti
Abstract: A framework in which fuzzy vaults are made to contain the audio and video of the users and the authentication is done through it but it is very difficult to build and contain all the user's data also continue monitoring can be carried out throughout the webinar.

**Methodologies:**

- Audio and video-based authentication

**Advantages:**

- It will ensure integrity of the webinars.

**Disadvantages:**

- No IP tracking
- Difficult to obtain fingerprints of all users

[6] Title: A palm print-based cryptosystem using double encryption.
Authors: Amioy Kumar, Ajay Kumar
Abstract: combination of both cryptography and biometrics where biometrics are captured and encrypted so if you have to break the biometric details and use them need to break the encrypted message and the get it hence double encryption technology is used to ensure the security.

**Methodologies:**

- Double encryption

**Advantages:**

- It provides the high security.

**Disadvantages:**

- There is no live IP tracking.

## III. METHODOLOGY

### 3.1 Socket Programming

Socket programming is a way for programs to communicate over a network using the internet protocol suite. A socket is a programming interface that allows two processes to communicate by packing and taking packs of data across the network.

To prompt a socket connection, a program must first generate a socket object and specify the protocol and address family to use. The address family can be IPv4, IPv6 or Unix. Once the socket is created, it can be used to transport and admit data to and from other sockets.

Socket programming can be used to implement colorful network protocols, matching as HTTP, FTP, and SMTP. HTTP is used to transfer web messengers, FTP is used to transfer lines, and SMTP is used to transfer dispatch dispatches. There are two types of sockets garçon sockets and customer sockets. A garçon socket listens for incoming connections from customer sockets, while a customer socket initiates a connection to a garçon socket. Once a connection is established, data can be transferred and entered between the two sockets.

Socket programming also includes colorful protocols and functions, similar as TCP, UDP, and elect(). TCP is a dependable, connection- acquainted protocol, while UDP is a connectionless, unreliable protocol. The select() function allows a program to cover multiple sockets for input and affair, and to perform different conduct depending on which socket is ready.

Socket programming is an important aspect of network programming and is used considerably in numerous operations, similar as web waiters, dispatch guests, and online games. It requires a good understanding of network protocols and computer networking in general, but can be a mighty tool for setting up networked uses.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

### 3.2 Reverse DNS

Reverse DNS (Domain Name System) is a process that involves the translation of an IP address into a domain name. It is also known as reverse mapping or inverse DNS lookup. In regular DNS, a domain name is translated into an IP address so that computers can communicate with each other over the internet. Reverse DNS does the opposite, providing a domain name from an IP address.

Reverse DNS is commonly used for spam filtering, network troubleshooting, and identifying potential security threats. It allows the recipient of an email to verify the sender's domain name and prevent spam or phishing attacks. Network administrators use reverse DNS to identify problems with their network and detect suspicious activity.

Reverse DNS is implemented through a system of PTR (pointer) records. PTR records are essentially the reverse of A records (which map domain names to IP addresses). PTR records map an IP address to a domain name. This mapping is stored in a special type of DNS zone called the in- addr.arpa domain.

The in-addr.arpa domain is used for reverse DNS lookups of IPv4 addresses. The ip6.arpa domain is used for reverse DNS lookups of IPv6 addresses. The in-addr.arpa domain is divided into different subdomains, each corresponding to a range of IP addresses. Reverse DNS is an important tool for maintaining a secure and reliable network. It allows administrators to quickly identify and address potential problems and protect their network from threats. It is also a useful tool for internet users who want to verify the legitimacy of emails and other communications they receive.

## IV. DESIGN

In the system architecture admin will create webinar and share the link. The admin will keep a track and monitor the participants activity. The admin is to only source to detect the all kinds of activity of the participants. He is having global authority of the webinar. If participants misbehave in webinar the admin will monitor such kind of activity and necessary action will be taken. The admin can trace the IP Address of participants so that he can know the details such as hostname, of that participant who is misbehaving. Basedon the details which has been gathered by the admin, he can block the participants IP Address so that participant cannot re-enter the webinar with that same device. The system architecture is designed such a way that admin is the one who takes care of the entire webinar and manage all the participants

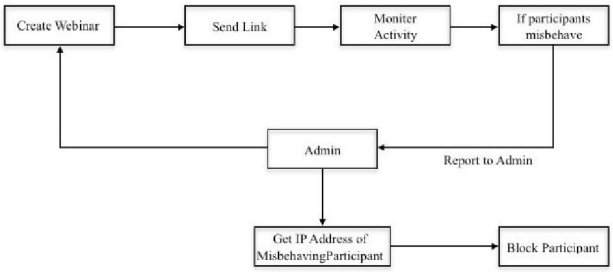


FIG 1: System architecture

## V. IMPLEMENTATION

The project is divided into four modules they are as follows:

- Admin is a super user of our project, Admin will create webinar meeting and monitor the activities of participants.
- Participants are the secondary user who will attend the webinars.
- Whenever a participants joins in a webinar admin will collect their IP address using the getremoteIP().
- Admin will be always monitoring the webinar sessions if any participants involved in malicious activities admin will block the participant from this webinar session.

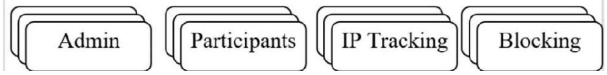


FIG 4:Modules of the project

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

## VI. CONCLUSION

When the world hit with the pandemic all the public gatherings has been restricted. Like a product, the webinars are shifted to the online mode via the conferencing application or through the web. Many techs have been focused on it and gave the product which can help people in the current condition. For the conduction of the webinar the application should provide the features with are needed by the people to conduct the webinar interactively. With the all-common features, the people expect their privacy so they focused on it to provide the well factored authentication security over the application. They have to focus on the people with fake id who are in intention to disturb the webinar. So, they came with the blocking features to specifically block the person who is disturbing via his IP So that the same person cannot join the respective webinar again

## VII. ACKNOWLEDGEMENTS

We would like to express our gratitude to SJC Institute of Technology, our college, we express our sincere thanks to **Dr. G T RAJU**, Principle SJCIT, Chickballapur for providing us with excellent infrastructure to complete the Project. We express whole hearted gratitude to **Prof. SATHEESH CHANDRA REDDY**, who is the respected HOD of Information Science Department. We wish to acknowledge his help in making our task easy by providing us with his valuable help and encouragement. It is our pleasure to thank our project Guide **Prof. Nagaraja G, Associate professor, Department of Information Science and Engineering**, SJCIT for his guidance encouragement and valuable suggestion from the beginning of the project work till the completion without which this project work would not have been accomplished. We express our sincere thanks to Project coordinator **Prof. ARVINDA THEJAS CHANDRA SJCIT**, **Associate professor, Department of Information Science and Engineering,** for providing us with excellence infrastructure to complete project

## REFERENCES

**[1].** Alotaibi, S. (2010). Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. The 4th Saudi International Conference, The University of Manchester,

**[2].** UK. Apampa, K., Wills, G., & Argles, D. (2009). Towards Security Goals in Summative E-Assessment Security. International Conference for Internet Technology and Secured Transactions, pp: 1-5.

**[3].** Asha, S., & Chellappan, C. (2008) Authentication of e-learners using multimodal biometric technology. International Symposium on Biometrics and Security Technologies, pp: 1-6.

**[4].** Chen, B., & Chandran, V. (2007). Biometric Based Cryptographic Key Generation from Faces. Proc. of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Application, pp: 394–401.

**[5].** Flior, E., & Kowalski, K. (2010) Continuous Biometric User Authentication in Online Examinations, Seventh International Conference on Information Technology, pp: 488-492.

**[6].** Monrose, F., Reiter, M., & Wetzel, S. (1999). Password Hardening Based on Keystroke Dynamics. Proc. of the ACM Conference in Computer and Communications Security, pp: 73–82.

**[7].** Rogers, C. (2006). Faculty perceptions about e- cheating during online testing. Journal of Computing Sciences in Colleges, 22(2): 206-212.