iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: ETPAM-2018 **Issue:** Conference **Month of publication:** March 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Chat Application Using IP Address with OTP Authentication

Mrs. G. Aswini[1]., Asha T[2], Aswini L

[1,,2,3]*Assistant Professor, Department Of Computer Sciences. Joseph's College of Arts and Science For Women-Hosur*

Abstract: ***Since the 1990s, two technologies have reshaped how we see and experience the world around us. These technologies are the Internet and mobile communication, especially smart phones. The Internet provides a cheap and convenient way to explore and communicate with distant people. A multitude of services have converged and potentially the most notable is social networking. With increased interconnectivity and use of online services, concerns about consumers' security and privacy are growing. At present, while the popularity of chat applications increases, this brings some security problems with it. In computer networking, IP address spoofing or IP spoofing is the creation of internet protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender . IP spoofing is a technique used to gain unauthorized access to machine. One client can hack the IP address of another client, but we can secure the IP address by giving an authentication that cannot hack the IP address of a particular client, which is chatting to the server. The secure connection between the client and server for chatting is authenticated by using IP security protocol with simulated IP address. This authentication process is done by sending OTP tokens from server and that OTP tokens is received by the client. This project has three steps. At first step, server has been identified the client itself to give OTP to the client from the server. The second step is called as connection and client connects to the chat room via OTP. The third step is messages from server/client are sent to client/server through two different IP Address. After few time intervals, it will get timeout.***

I. INTRODUCTION

Information security is a primary goal for chat application and achieving information security may provide a healthy chat. Consequently, information systems are continuously developed that aim at providing safe data storage and communication between working units of the organisation involved. The development and expansion of the Internet have established it as one of the most important communications channels both at the level of large scale organisations (banks, multinational companies etc) and at the level of simple users.

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further Internet Protocol Security (IPSec) is a network protocolsuite that authenticates and encrypts the packets of data sent over a network. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session. IPSec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPSec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPSec supports network-level peer authentication ,data-origin authentication, data integrity, and data confidentiality (encryption), and replay protection. Authentication Header (AH) is a member of the IPSec protocol suite. AH guarantees connectionless integrity and data origin authentication of IP packets. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets.

There are numerous applications available that allow for real time chatting over the internet. The purpose of this project is to implement a java based client/server chat application connected through IP address with OTP (One Time Password) authentication. The authentication of people is used in almost all areas of human activity. To chat with client and server user needs to generate OTP (One Time Password). OTP is a password that is valid for only one login session on a computer system. Whenever server runs,

©IJRASET (UGC Approved Journal): All Rights are Reserved

it will wait for a client connection and when the client runs, it will ask an Id. After entering the ID, the server will generate the OTP password for that particular ID. After entering the OTP it will verifies the OTP and log into the chat application. In this chat application, server will have a different IP address and client will have a different IP address. This project is made up of two different application that is client application and server application over the internet. The user can simulate the IP address of a single system. To start chatting, the client should get connected to server via IP address. The aim of this project is to secure the chat application. While client server chatting a time limit given to stop the chat.

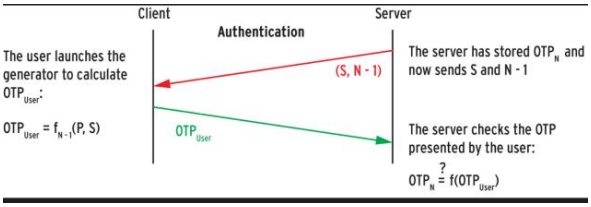


Figure 1:generating OTP

II. CONCLUSION

The main objective of the project is to develop a Secure Chat Application. I had taken a wide range of literature review in order to achieve all the tasks, where I came to know about some of the products that are existing in the market. I made a detailed research in that path to cover the loop holes that existing systems are facing and to eradicate them in our application. In the process of research I came to know about the latest technologies and different algorithms. I analyzed HMAC based One Time Password algorithm (OTP), authentication and I had implemented those functionalities in my application. As a result, the product has been successfully developed in terms of extendibility, portability, and maintainability

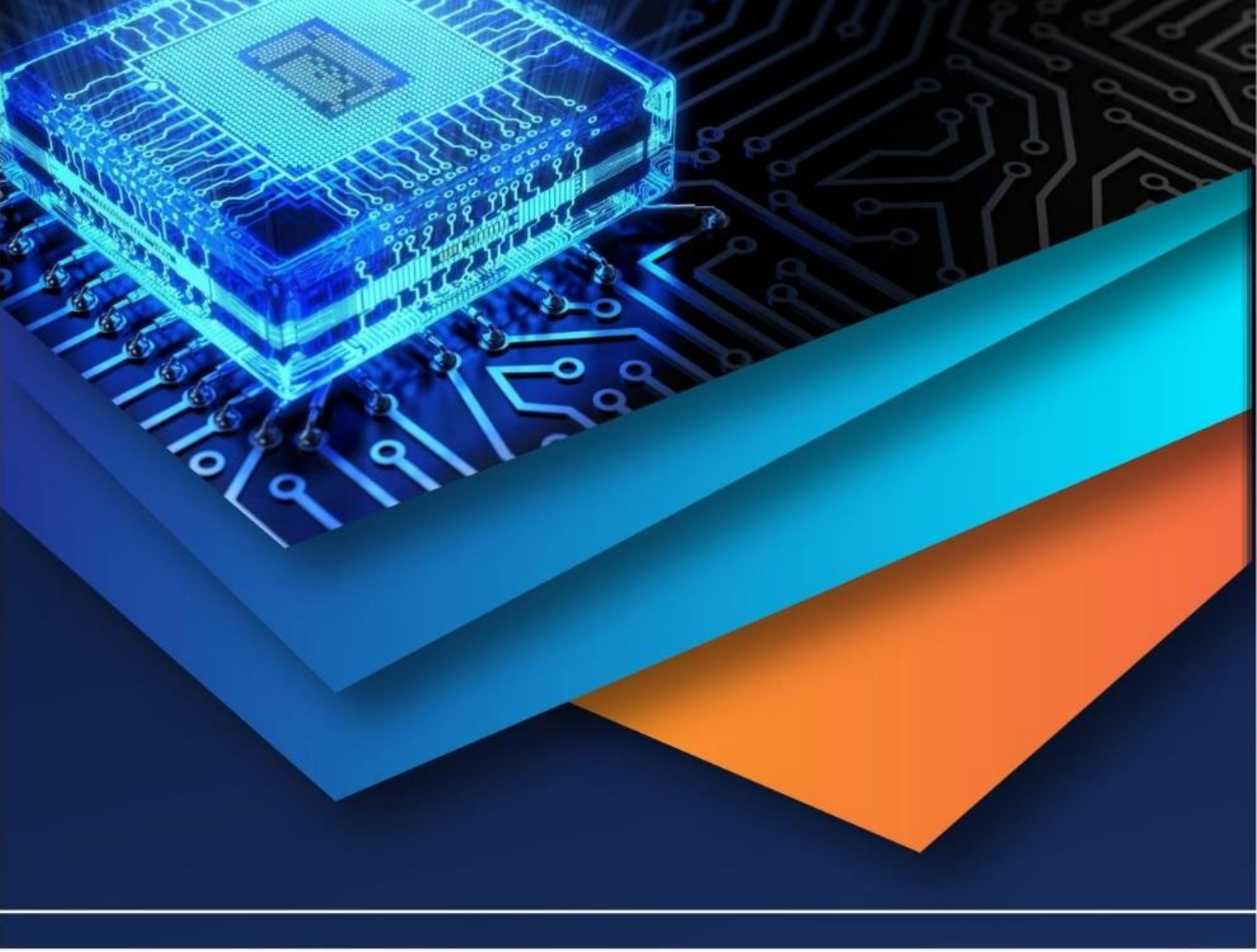
III. FUTURE WORK

With the knowledge we have gained by developing this application. I am confident that in the future we can make the application more effectively by adding this service. We will make the chat application between single server and multiple clients through IP address in the single system. And we will try to provide the authentication do not hack the IP address.

REFERENCES

[1] Java 2: “The Complete Reference”, 5th Edition by Herbert Schildt.
[2] Core JAVA. Fundamental Concepts.
[3] Core Java, J2EE, JSP, Servlets, and general programming concepts.
[4] The Advanced Java, Swing e-book covers advanced Java Swing topics.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)