Modulation of security and speed of data for VPN network based on Indian server

[1]Sourabh kothale, [2]Kamanshu patil, [3]Namit Khobragade, [4]Sumeet Gupta, [5]Akshay Chandekar
[1]Student, [2]Student, [3]Student, [4]Student, [5]Student
JD College of Engineering

***Abstract* - In this paper a pipelined architecture of the highest speed of security of data transfer and security when the is encryption and decryption. The NSP finds in application in Virtual Private Network, e-commerce and in so many filed that data confidentiality. VPN is mostly used in so many enterprises and company, in the security of data transmission. VPN have the encryption and privacy, but the VPN has increased the intensity of data encryption. In day to day life, the people on mobile devices are using the Internet. The amount of private information is gathering by people's devices**

***keywords* - VPN, Tunneling, Private**

I. INTRODUCTION

In this day, we are currently facing the ever-changing form of technology and we are required to protect our data from the internet or from the people who are trying to get our data for their benefit and hence we are working on a technology to prevent it from happening and we are trying to protect our users identity by using our VPN server. Our VPN server will give users a secure connection to serf freely all over the internet while in a protected zone. Our VPN can be used to serf restricted sites with ease and in our paper, we are currently using more secure algorithms to give better experience to our user and by modulating the transferring speed of data packets in transport layer we are trying to increase the speed of our VPN by twofold that of the present technologies.

Current technologies are unable to coup up with the needs of current users demands for an application which is secure, fast and easy to use. Some VPN services are based on the security and can neglect the fact that this is a changing world and require a fast VPN service to get their result with more speed than usual application our currently using application. In this paper, we will be going to show the use of the latest algorithms like SHA-256, DES and some latest tunneling technologies like L2TP, P2P etc.

Our project will work on the privatization of data while blocking all attempts of stealing data from our user by giving our user a safe environment to work on and we will give them a sense of freedom that they can whatever they want without worrying about their data or their work data is being watched by other personals. Our VPN not only protect their data from attackers but also will give them a surety that their personnel details cannot be watched by us also in spite that their data is stored in our database we also cannot just browse through their data even if we want because of the hashing technologies that will work in between server and database the data that is to be extracted from the server will go through the hashing technology will be encrypted before entering the database and because of this technology we can proudly say even we will cannot have access to our users data.

II. METHODOLOGY

We will be implementing a system or more precisely we will create a server for our users to serf securely through the internet without the threat that their personalized data will be accessed by the other without their consent. The user will follow through following steps or more precisely will use the following method to get their desired outcome. User will install our VPN application. Application is window based created by using PHP technology and can be installed on a desktop. User needs to open our VPN application and sign-up.

Sign up procedure normally include inputting basic details such as email, username, date-of-birth. If the user is already registered then he can click on login button. He has to put his credentials like username and date-of-birth and log in. When a user first time signs up, he is asked about verification of email. After verification, the user's account is successful activated. Once a user logs in he is presented with a list of servers. From this list, he has to choose a preferred server he wants to connect to. But the preferred server or the basic server will be that of INDIA as we are focusing on Indian mass for our VPN.

Once the user selects the server then 'you are successfully connected ' message appears on the user home screen. The user is connected through tunneling protocol like L2TP etc. His data is transmitted from the VPN server Users IP address is now masked.

All the website can now see the IP address of the VPN server and user is now secure and their credentials are well protected by latest hashing techniques like SHA-256. Every data user send is first being sent to the VPN server in an encrypted manner and then the server forwards that message with its IP address. This way user's privacy is being protected After the user's session is complete user logs out from the application.

Once he logs out a message saying you are disconnected is shown. A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more.

Tunneling encapsulates your data into standard TCP/IP packets and safely transfers it across the internet. Because the data is encrypted, hackers, governments, and even internet service providers cannot see or gain control of your information while you are connected to a VPN server.

VPN allows users working at home or office to connect securely to a remote corporate server using the routing infrastructure provided by a public inter-network (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server.
An IPsec client VPN requires a VPN client software to be installed at the client's endpoint to be used in connecting to the main servers. A clientless SSL VPN.

However, uses any web browser to connect to the main office servers. The problem with the SSL VPNs is that they don't support applications that can't be run through web browsers. The flow of our project will be like given below and to understand more about our project a basic algorithm the basic algorithm .

Algorithm:

Step 1: START
Step 2: Register user
Then fill all required fields
a) User Details
b) Username
c) E-mail Address
d) Date of Birth (only month and year)

After submitting the user's data will save into our database after being hashed
Step 3: Log In

```
If (New User)
                {
                        Then go to Step 2
                }
        Enter user name and password

 If (Field is empty)
        {
                Then throw warning
        If (Field is not valid)
                {
                        Then throw warning
                        If (matches)
                        {
                        Open home screen
                        If (server="selected")
                        {
                                Connected
                                User Session Start;
                        }

        After surfing User can disconnect the server.
                        else
                        {
                        Automatically after 120 sec Session will stop;
                        }
                }
        }
```

Step 4: END.

The work-flow of our project can be pretty much understandable by the given algorithm. In our proposed framework the user is required to create a login ID to gain a private space he needs to have a working email because during the registration process the email needs to be verified.

SHA-256

SHA-256 IS stands for secure hash algorithm-256 bit and is a type of hash function which is commonly used to encrypt the data. A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It's like a formula or algorithm which can take the plain text and the SHA-256 algorithm
convert plain text into the hash and then that hash is a fixed length that is 64byte which represent the fingerprint of the data.

The input data can be any data, whether it's the entire Encyclopedia Britannica, or just the number '1'.
A hash function will give the same hash for the same input always no matter when, where and how you run the algorithm if you change the single word the meaning that word will change and respectively the hash function will be change.

Also, a hash function is a one-way function, thus it is impossible to generate back the input data from its hash. So, you can go from the input data to the hash but not from the hash to the input data.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support Virtual Private Network (VPNs) or as part of the delivery of services by ISPs. The entire L2TP packet, including payload and L2TP header, is sent within a User Data-gram Protocol (UDP) data-gram. A virtue of transmission over UDP is that it avoids the "TCP meltdown problem". It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LNS waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP session (or 'call') is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorized as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel. L2TP allows the creation of a virtual private dial-up network (VPDN) to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network

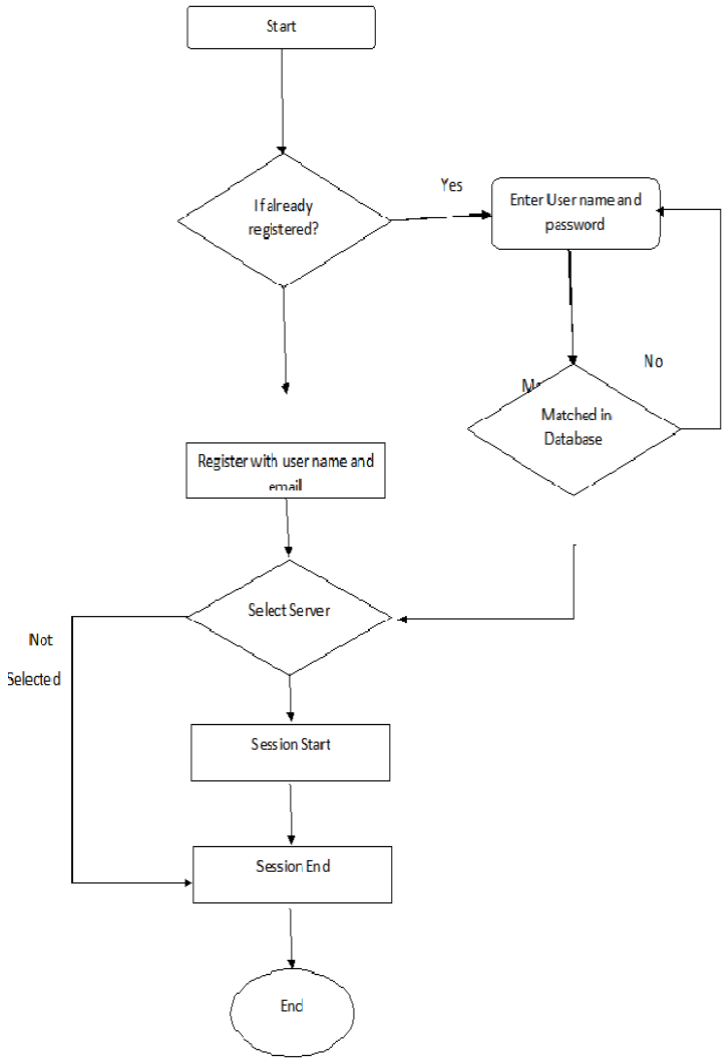

Fig: - Flow Diagram

III. CONCLUSION

The proposed system addresses the problems or limitation of current and use that to make it more user-friendly and reliable than most. It will be secure than most and faster than those systems that are currently in use. It will give utmost privacy possible.

IV. REFERENCES

[1] A stack-vector routing protocol for automatic tunneling, Simon Lassourreuille, acm, 24 Jan 2019.
[2] Protecting User Privacy: An Approach for Untraceable Web Browsing History and Unambiguous User Profiles, Ghazaleh Beigi, 23 Nov 2018
[3] DTLS Performance – How Expensive is Security?, Sebastian Gallenmuller , A Scalable VPN Gateway for Multi-Tenant Cloud Services, ACM SIGCOMM Computer Communication Review Volume 48, January 2018
[4] A NEW APPROACH FOR THE SECURITYOF VPN Kuwar Kuldeep V V Singh ICTCS '16, March 04-05, 2016