ISSN No:-2456-2165

Secure +, An Intrusion Detection System

Ankith Rai[1], Jovita Dsouza[1], Edison.C.Saldanha[1], Keerthana Raviprasad[1], Vasudeva Pai[2], Dr.Karthik Pai B H [2]
[1]UG Student, Department of Information Science and Engineering ,
[2] Professor, Department of Information Science and Engineering NMAM Institute of Technology,
Nitte, Udupi, Karnataka, India

Abstract: - Network security is one among the first essential perspectives to examine once working over the net .local area network with distinctive strategy. Regardless tiny or huge the market is, till now there is no secured network that is resistant to strikes on network, a stale economical secured network framework is crucial to protective shopper information. Risk of the business of becoming a victim to data sabotage and theft can be reduced by using a good secured networking system . The proposed system will overcome the difficulties in the Routers deployment which may unsuccessful in sending spoofed IP packet due to various reasons. The IP spoofing is carried out mainly by attackers using a Virtual Private Network to intrude into somebody's personal account. This project is designed to analyse packets and determine the attacker legitimate IP address thereby displaying used browser by the intruder to the do the same. The real time communication between browsers is achieved through WebRTC. However, if this system is implemented, it will highly facilitate in securing the user's data from getting intruded and will also explicitly display the location as well as the IP address used by the intruder to perform his actions.

Keywords*: - Web Application Security, Browser Security, AWS Cloud*

I. INTRODUCTION

Security in Network consists the policies which practices to stop and look for unauthorized access, misuse, modification, or any denial of a network electronically and through network-accessible resources. Security in network involves the knowledge of authorization to access in an exceedingly better network, that is been controlled by the network administrators. Users can select the area unit which is appointed in associate with ID. Different data authentication which will enable the users to access the information and the programs within the dominance. Secured network widely covers the stretch of personal computer networks, each personal and public, that area in unit will be utilized for day to day jobs, The job of conducting communications as well as transactions amid the businesses, the people and government agency. Networks can be personal, like amid an organization, which are publicly receptive to access. Security in network is concerned in the organizations and the different styles of the establishments. As its title explains that: It is used to secure the network, and additionally as to provide overseeing and protective operations that is being carried out. The most regular and simple manner of protecting a network device is by assigning it in a distinctive name and a corresponding release. Initially security of a network deals with the authentication, which is with a username. This needs to have only one detail of authenticating the user name—i.e., the password—this is typically the one-element authentication. With the two-element authentication, Additional to this the user has used (e.g., a mobile phone , security token); Once all the parameters are verified, a security through network impose the control policies relatively like for what services in the specific area are allowed to be acquire by the users in the network when user logs into any websites. Though this technique is effective to stop the uncertified access, this element could be unsuccessful to examine the doubtless dangerous contents like personal computer worms or viruses like Trojan virus which is being transferred through network. The software like Antivirus or a IPS (intrusion prevention system) helps in detecting and inhibiting the action of such type of attacks if occur. An exception intrusion recognize system can also used to monitor the connection like wireshark traffic and can also be logged for probe functions and for the higher level analysis. The advanced systems consist of combined automatic machine learning which analyse the traffic in network and find agile attackers who attack network from malicious internals or external attackers that are compromised with a user accounts or machine.

II. LITERATURE SURVEY

A. File Storage

When we are using one computer in an office the best way to think about data is by storing them in files and folder..The file systems are built as it uses the folders to arrange our data. Since the advancement in technology, and use of multiple device, and sharing and accessing our data across all the device. This is the reason why, the traditional approach of data stored as 'documents' in drop file 'folders' when there is multiple operation on same file at same time in different device then it breaks down it. The object storage, which later was redesigned in advanced way that it should dismiss the existing current data in an organization as well as the standard like allowing to put one folder in another or giving access to only a one person for editing a file at a particular time. It serves everything as a bit of the information, coordinate with each and every other pieces of data. The object storage systems allows to share and store the information over the many computers. there are still some user who are using cases for file storage as the experts. For example, this is best fits for small-scale organization to have local storage that needs to be uncommonly fast. Generally object storage doesn't work well in that conditions because the cluster in object storage is on the other side of a connecting network.

B. IP Detecting Technique

➢ *Probabilistic Packet Marketing*

Stamping parcels with the switch's IP address, breaking down demonstrates that all together or to pick up the right assault way with 95% precision upwards of 294,000 bundles are required. The second methodology is that, the edge checking, necessitates for the two hubs that together make up an edge marked providing way to their IP addresses alongside making the disconnection between them. This is the methodology that would require more state data in every one of the parcel than straightforward hub checking however would merge a lot quicker. Three different ways are recommended to diminish the state data of these sort of methodologies into something increasingly sensible. The primary methodology is to XOR every hub shaping a border in the way with the one another. Hub A supplements its IP address into the parcel and even sends it to the hub B. It Being distinguished at the hub B (identifying a 0 out there), B consequently XORs its location with the Location of hub A. The new dimension of information element called as an id of edge and diminishes the required condition for edge inspecting it by half. Their succeeding methodology is to additionally take the edge id and section it into the k littler parts. At that point it is haphazardly chosen a part and encoded it, alongside the section balance so the right relating piece is chosen from a downstream switch for handling. At the point when the enough bundles are gotten, the unfortunate casualty can recreate the majority of the edges the arrangement of parcels crossed (even within the sight of numerous attackers).The most number of blends are needed to modify a divided id of edge, so the remaking of a assault chart is escalated computationally by specialists. Moreover, the methodology results in countless positives. For a model, with just 25 assaulting hosts inside a DDoS assault the recreation procedure take large number of days for the construct and results in a huge number of the false positives.

➢ *Deterministic Packet Marking*

Here they explained sensible topologies for the web that it consist of ASs and LANs with a connective border and attempts to include a sole mark on the packets which are inbound at the network ingress point. The idea is to include, irregular probability that is .5, the lower or upper half of the IP address of the access interface within the packet of fragment id field, and then they set a stock bit in a such a way that it indicates that which part of the address is situated in the shred field. Using these type of path they plea that it's possible to gain .99 probability of 0 false positives just after 7 packets. In another possible approach the IP address is encoded into 16-bit hash that of address of IP. First of all at start selecting of a familiar hashing function is done. They describe that if there are edge routers which are greater than 2^16 then there would be some collisions. They worked on to reduce the problem of collision by proposing new technique in which selecting of random distributed hash function from a global set, and further it is enforced it to the IP address. In the either scenario of hashing, the hash as well as the source addresses are summarized together in the chart for later confirmation along with a bit that indicate which part of the received address. Even though this is a sophisticated procedure and a irregular hash selection, they have ability of decreasing the collision of address. Using this deterministic method the time for reconstruction of procedure for the mark is reduced. By making mark to be encode through the hashing they propose the probability of collisions, and that is why it's false-positives.

➢ *Router-Based Approach*

With the switch based methodologies, the switch is been accused of the keeping up data in regards to bundles that go through it .In their first methodology The thought proposed is to create a unique mark of the parcel,in light of the fixed pieces of the bundle (source, objective.) and the underlying 8 bytes of payload (which have a low likelihood of impact). in particular, free straightforward hash works each creates a submit in the scope of 2n-1. Then a bit is to set at the file which makes to produce a unique finger impression when joined with the fixed of all the other hash capacities. All of the fingerprints are secured in a 2n bit table for later recuperation. The space genuinely necessary at every switch is restricted and controllable (i.e,2n bits). A small n makes the probability of accident of package hashes (and the counterfeit ID) higher. At the point when a bundle should be followed back, it is sent to starting switches where unique marked matching are checked. As the time goes on, the unique mark data is "thrashed" by the hashing that created by different bundles. Along these lines, the choice for this methodology debases with the time that has gone between the section of the bundle and the follow back cross examination. In their another methodology, they had wish to incorporate the SPIE approach with the methodology of chronicle the 2 layer interface identity alongside the system identity (Virtual LAN or genuine identity), the Media Access Control address of the 2 layered switch that has got the parcel and also the connection identity it came in on. The data which received is then made to put into two look-into tables – with both having the switch (2 layer switch) Media Access Control id for progress. They totally depend on the Media Access Control: port as a strategy for following a parcel back (regardless of whether the Media Access Control address is been imitated). Helping them to alleviate the issue of the capacity constraints the hashing approach is used and usage (SPIE) –which alters to acknowledge their data in order to be hashed. They grant their calculation is moderate way (O(N2)) and with just 3 millions hashed package is been put away to the inexact time before the condensed tables are shows the invalid within one minute. This helps in directing any assault reaction that should be ongoing – the probability just on one-authoritative Local Area Network space.

III. PROPOSED SYSTEM

The above mentioned technique in literature survey are effective techniques where probabilistic packet marketing checking spread of the addresses of conceivable switch messages over a range that is unreasonably huge for the attacker to effortlessly make messages that slam into genuine messages.Deterministic packet marking uses the detection engine that considers the characteristics of the parcels to distinguish changing single sites including DDOS assault Router-Based approach uses the delay time when receiving the packets to the other end of the router, all these techniques are used to find out IP address but ours proposed system too finds the Local IP as well as Public IP even if VPN is used.

A. Technique of WebRTC

WebRTC allows web apps to create Peer-To-Peer communication. WebRTC uses Peer-To-Peer communication as well as and NAT Traversal.

➢ *Peer-To-Peer Communication*

If a person want to convey any information with another user by using a web browser, then web browser of each and every person must go through some of the following steps that is first the user should Agree to start with a communication, then the user must know how to locate one another . Bypass in the security lets to Transmit all hypermedia communications in the real-time world. The big challenges being associated with that of the browser-based peer-to-peer communications is to know the technique to locate and also to build a secure network connection with that of any other browsers in order to bidirectional send data from one system to another.

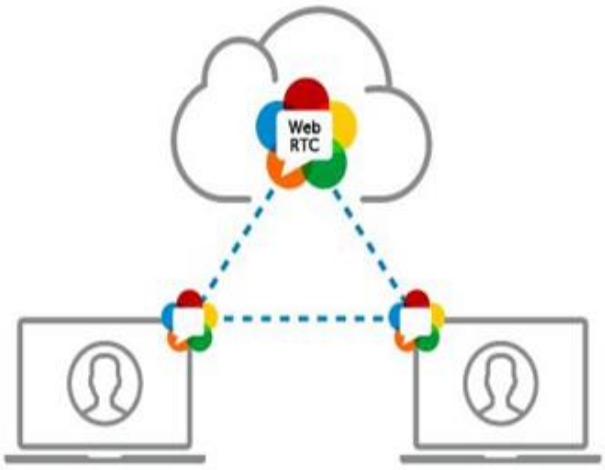

Fig 1:- Communication between Two Different Users.

➢ *NAT Traversal*

The system which you are utilizing doesn't commonly have a static open IP address doled out. The explanation behind this is your PC is sitting behind a firewall and a system get to interpretation gadget (Network Address Translation).A Network Address Translation device is a device that decodes a private Internet Protocol addresses from inside a firewall to open standing up to Internet Protocol addresses. Network Address Translations devices are required for security and IPv4 imperatives on available open Internet Protocol addresses. That is the reason your web application shouldn't expect that the present gadget has an open static Internet Protocol address. This is the means by which a Network Address Translation gadget works. In the event that you are on a corporate system and need to join the Wi-Fi, your Personal Computer will be appointed with an , in any case, your Internet Protocol address may look like 164.43.17.58. The outside world is able to see your solicitations as originating from 164.43.17.98 however the Network Address Translation gadget will guarantee that the reactions to the solicitations, performed by your machine will be sent to the inside, 172.0.23.4. This occurs because of mapping of the tables sequentially. Note that not withstanding the IP address, a port is additionally required for system interchanges. In the event that the contribution of a Network Address Translation gadget is available, your program needs to make sense of the Internet Protocol address of the machine, which has the program you need to speak with. This is the place the Session Traversal using Relays around Network Address Translation(TURN) and Traversal Utilities for Network Address Translation (STUN) servers come into the image. All together for WebRTC innovations to work, a solicitation of a STUN server first made for open to confronting IP address. It is acting like as if your PC is making an inquiry to a remote server, which is made to ask what the IP address is when it gets it in the question from. The remote server at that point reacts with the IP address when it sees. Accepting this procedure do works well then you get to know your open confronting port and IP address, you then you are ready to advise different friends on associating with you straightforwardly. These companions are additionally ready for doing something very similar utilizing a TURN or STUN server can disclose to the user what address to get in touch with them at also.

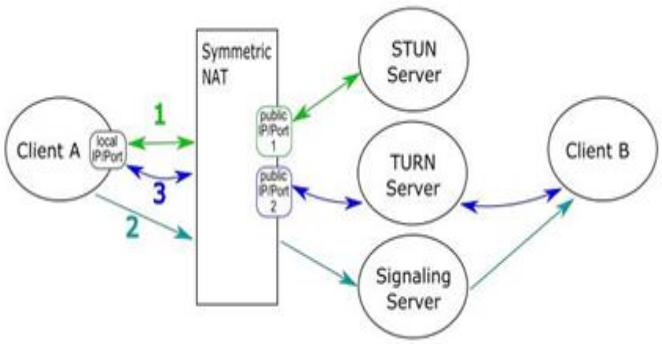

Fig 2:- NAT Traversal

B. Browser Fingerprinting

"A machine, device and browser fingerprint is the data or information collected through the remote computing device for the purpose of identification the system. Even when cookies are turned off individual users can identify the fingerprints fully or the partial of the device. What it tells that, when the users are connected to the network on the particular users smartphones or laptops, the users device hands over a certain amount of data to the receiving server

about the websites that user is visiting. The browser fingerprinting technique is so strong and also a effective method that the websites uses this for gathering the data about the user using the particular browser with the type of browser and the version, with the users operating system, language, timezone and also the other active settings. These gathered data seems to be nonspecific at first when viewed and there's no necessity that it must look modify for one specific person to identify.Anyhow, there can be a chance for a another user who can have the 100% of matching the browser information. The panopticlick study detected that only 1 in whole of the 2,86,777 other browsers available will be sharing the same fingerprint as that of the another user. Sites really utilizes the data given by programs to recognize the special clients and track their online conduct occurring. This procedure is a program or gadget which uses unique finger impression is a term used to portray an identifier created from data recovered from a solitary given device so it is very well utilized to recognize that solitary device as where it is present.whenever the user is viewing the website a unique browser fingerprint is generated with the identifier.Identifier will be same even if the cookies are cleared.The identifiers are generated for the users particular device or the browser.A program unique mark (browser fingerprinting)is created from the programs client operator, timezone counterbalance, accessible textual styles, language and many more.To produce a program unique mark (browser fingerprint)first you should have JavaScript empowered as it is the least demanding approach to accumulate the vast majority of the data about a browser. Access javascript gives us the things to be viewed like users size of screen, language used, time zone , and the other features too [2]. The gathered information is collected together in a string and then it is further hashed to generate the identifier, more the information you are able to gather about a single browser the more browser. When that it unique fingerprint mark will generate with less collision.A large portion of the sites for the most part have their clients make record and sign in previously permitting them access to bits of the site. Where program fingerprints particularly helpful for attempting to distinguish mysterious guests to a web application.

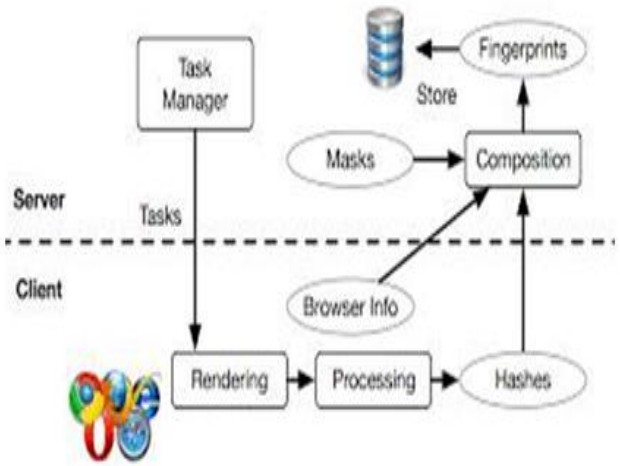

Fig 3:- Stages of Browser Fingerprinting.

C. AWS Cloud with Encryption for File Storage

Amazon Web Services has been used as a cloud provider for storing user files. Amazon Web services can be integrated with the django app via boto3 library We make use of two services of AWS1) S3 Storage (S3 stands for Simple Storage Service) We create one bucket which is an instance for storing files. The files that are stored will be the static files (css,js) , user profile pictures as well as the user's personal files. Further, we make the profile picture folder in the AWS bucket to be public since it needs to be shown on our page. User personal Files can be encrypted via AES 256 encryption or via Amazon's Key Management Service which uses the TLS (transport layer security) protocol.2) IAM (identify & access management) In order for the our Django apps to be connected to AWS service, we need to supply the AWS access ID and also AWS secret access key (which is produced only once) to the settings file in the main project folder. This is generated in the IAM service. Further, these keys are the only means of decrypting the files on the cloud for Amazon's KMS encryption. The keys are stored as environment variables in the Admin's computer and hence cannot be disclosed unless having access to the Admin's PC.

IV. IMPLEMENTATION

A. Client Registration

A website is created using django framework to store the files of the particular registered user where first the user must have to be registered to the particular webpage with credentials such as Name, Password and email address, then once the user has registered to the particular website it then directly takes the user to the login page where user tries to login with name and email in order to go to his/her's particular profile to upload the files.

B. Client Login

When a registered user tries to login to the webpage what happens is that the browser fingerprint ID which is unique is obtained and stored in the database which is concatenated with the user name and browser Fingerprint ID so must be unique if any other client registers to the same website using same device the registered user tries log in into the website again using the same device the system then compares the username with the username which is already stored in the databases and then grants the permission to access to the particular users profile where along with the file upload with encryption it has some additional functionalities like changing the profile picture as well as password reset via gmail.The security to the file is provided through cloud encryption.The database Postgres Sql is used to store the credentials of registered users.

C. Intrusion Prevention

As we know that it gives access only to the registered user with same device used but When a particular registered user tries to log in to the website from another device, a message via email is directly sent to the user along with the public as well local IP address saying that intrusion is detected with the password reset link ,Browser details as well as Geo-Location .If at all some other person

knows the username and password and tries to access using other device this feature of sending mail warns the particular registered user so that no one except the trusted user can log in.

V. RESULTS

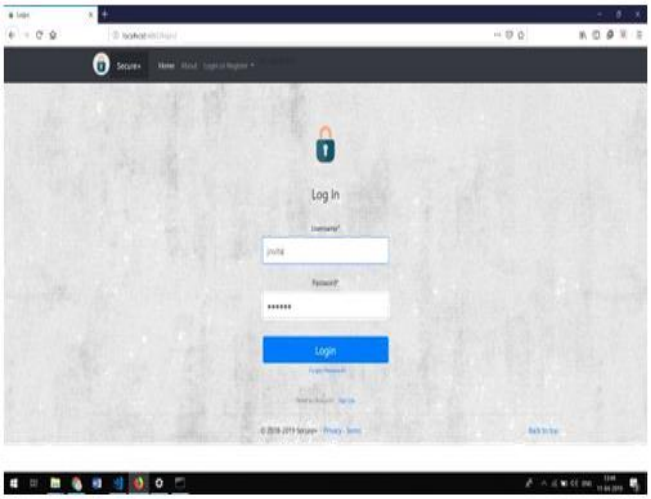

Fig 4:- Users Login Page.

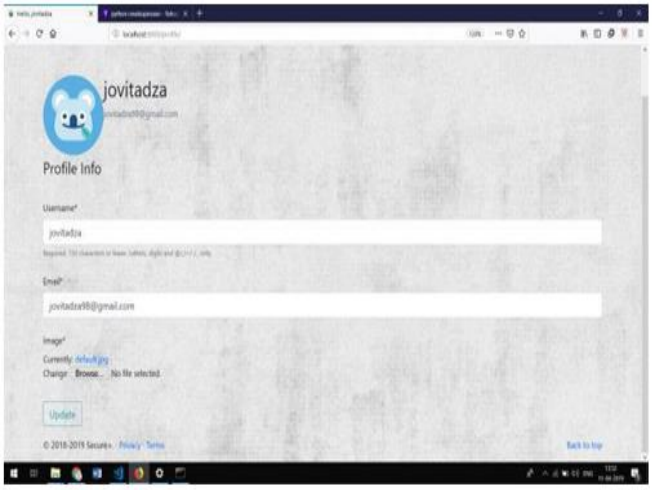

Fig 5:- Users Profile.

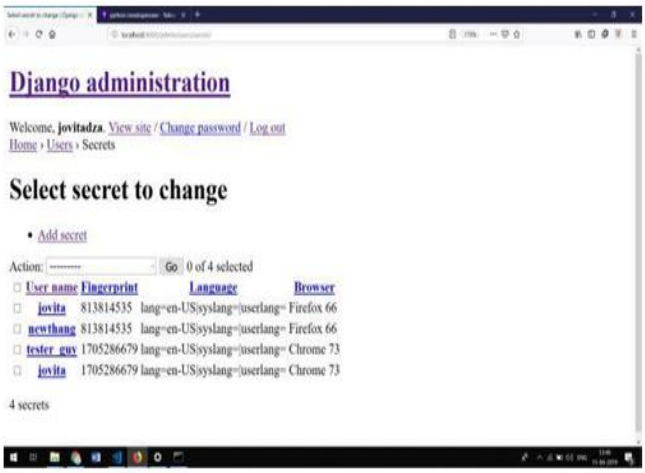

Fig 6:- Device Details of All Logged in Users.

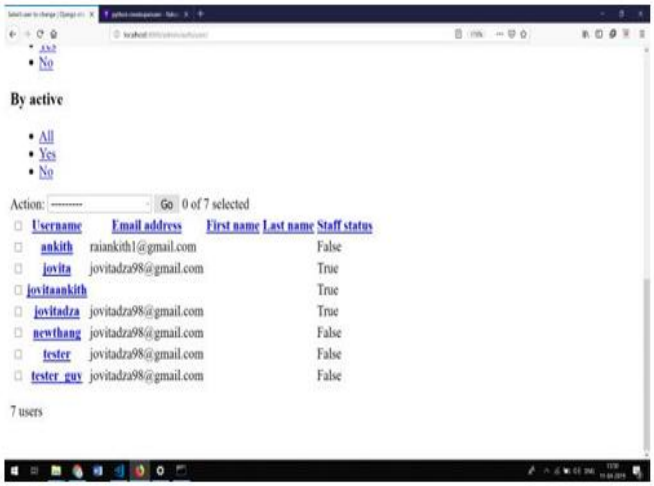

Fig 7:- Registered User Information Stored In Database.

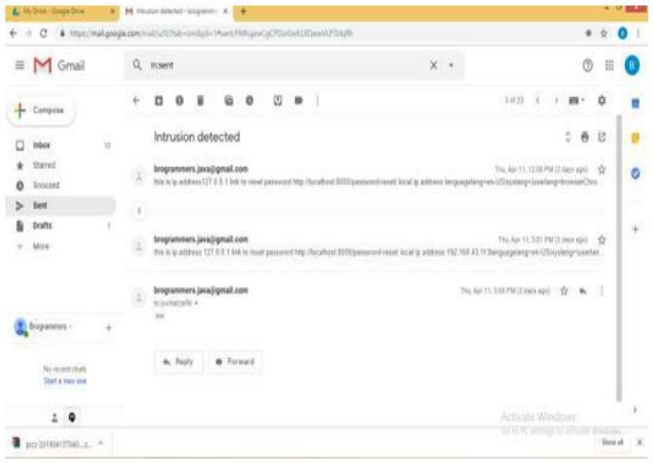

Fig 8:- Email Sent To The User Along With IP.

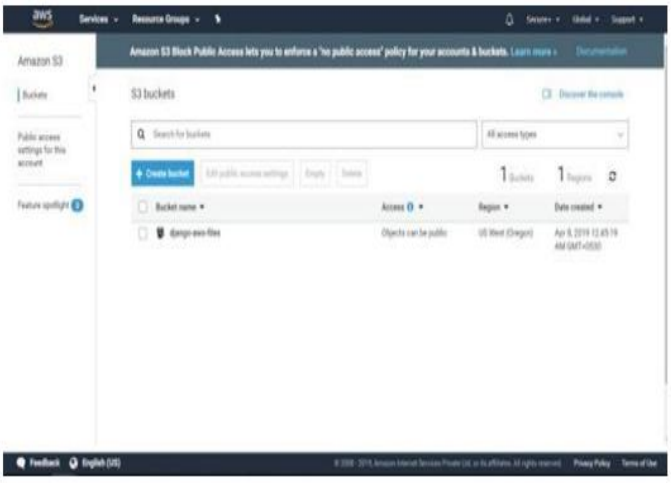

Fig 9:- S3 Bucket Name.

Fig 10:- AWS Home Page.

VI. FUTURE WORK

➢ *Public IP for VPN Enabled System with Geo-Location*

In our proposed system if an attacker uses the VPN enabled system to intrude the Website then the Local IP , Browser Fingerprint along with Browser Name, Language is found out but the public IP address and location of the attacker cannot be found in our proposed system. Even the details of System OS with User-Agent can be found out.

➢ *Geo Location System with VPN*

Intruder uses VPN in order to hide their actual location by hiding the real IP address when trying to access other users information illegally but if the intruder uses this particular website the local IP address can be found out but the location of the intruder cannot be found out as of now using Geo Location as the intruder is using VPN .Further more development in project must be done to find out the location even after a intruder uses the VPN and tries to intrude by deploying into heroku.

➢ *File Modification on Cloud without Retrieving*

The file storage system that we provides includes storing files in AWS cloud but when if some modification needs to be done to the file ,first the file must be retrieved from the cloud and then there the modification is made to the file ,after all the modification done again the file needs to be uploaded to the cloud. Further more what can be done is that ,the method of modification in cloud itself without retrieving the file can be implemented.

REFERENCES

[1]. Liu, Xiaofeng, Qixu Liu, Xiaoxi Wang, and Zhaopeng Jia. "Fingerprinting web browser for tracing anonymous web attackers." In 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), pp. 222-229. IEEE, 2016.

[2]. Nair, Krishna V., and Elizabeth RoseLalson. "The Unique Id's you Can't Delete: Browser Fingerprints." In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1-5. IEEE, 2018.

[3]. Bracci, Fabio, Antonio Corradi, and Luca Foschini. "Database security management for healthcare SaaS in the Amazon AWS Cloud." In 2012 IEEE Symposium on Computers and Communications (ISCC), pp. 000812-000819. IEEE, 2012.

[4]. Gouaillard, Alexandre, and Ludovic Roux. "Real-time communication testing evolution with WebRTC 1.0." In 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1-8. IEEE, 2017.