REAL TIME DETECTION OF HYBRID AND STEALTHY CYBER-ATTACKS IN SMART GRID

Ishu Jugran [1] , B.V Nagasai [1] , T.Malathi [2]

[1] Student, Department of Computer Science and Technology, SRM Institute of Science and Technology, Vadapalani, Chennai,India

[2] Assistant Professor, Department of Computer Science and Technology ,SRM Institute of Science and Technology, Vadapalani, Chennai, India

Abstract:

The concept of security to a network has been introduced when the engineers found unauthorized and obscure people of society tried to damage the network or modify the network without the respective owner's acknowledgement, since that network security have been evolved in a vigorous rate and at the same time the technology for breaking a network's security also increased at a rapid speed simultaneously. Since we people rely on internet completely on a regular basis , security should be robust as powerful , so since the existing system of file sharing is compromised we intend to propose a new architecture which is effective than previous architecture. We provide a file sharing method and our main goal is to find the respective obscure people who try to damage the network, as we all know a user can try multiple attempts over a password field and a hacker can make this excuse to guess multiple passwords and decrypt the password so that he can damage the data , we made an system which will provide the admin of an website to get details of the person who enters the wrong password with his Internet protocol address with his latitude and longitude position and his ISP so that we can easily find out the person who tries to damage the network. Since the existing system mainly concentrate over DDoS (Denial of Service) attacks using IP trace back which is an effective solution but still it have its disadvantage which should be rectified , and we provide a novel cloud based architecture which will be using forensic trace back which is effective comparatively to the existing architecture by implementation of FACT.

Keywords: Network Security, DDoS , IP Traceback, FACT

1. Introduction:

In the concept of network security there has been many concepts evolved for securing the network and at the same time for breakage of network anonymously, so since the network security at its peak it still have its data leakage breach and it cannot successfully trace back since hackers evolved so much since using anonymity in a smart way , one of the major possibility of trying to login as a user can be prevented at the first place using our architecture, since a hacker can try as many as possible trial and error method in a login panel we usually will not recognise as an attempt , but this is where we can recognize an attack pattern , so using this we are trace backing our respective hackers IP when one wrongly enters the password , we can get his ISP , IP address and his geo location using longitude and latitude so that we can block him in an effective and in quick way. This architecture works on AES algorithm for random cipher text generation since it is more effective to decrypt comparative to other algorithms so that the user who is going to download the file have to enter the cipher key generated by system at the time of uploading the file so that only the authenticated person authorized by the data owner can download using key , we are using a novel cloud based architecture for trace backing IP referred as FACT. The existing system IP traceback is a compelling answer for recognize the wellsprings of bundles just as the ways taken by the parcels. It is for the most part propelled by the need to follow back system interlopers or aggressors with satirize IP addresses, for attribution just as assault barrier and moderation. For instance, traceback is valuable in shielding against Internet DDoS assaults. It additionally helps with alleviating assault impacts; DoS assaults, for example, can be moderated on the off chance that they are first distinguished, at that point followed back to their starting points, lastly hindered at passage focuses. Furthermore, IP traceback can be utilized for a wide scope of common sense applications, including system crime scene investigation, security evaluating, arrange blame conclusion, execution testing, and way approval. It have its own disadvantage of trace backing technique to discover ISP's mechanism and drawback of distributed logging is the lack of properties favoring partial deployment.

2. Literature survey

From [1] we become acquainted with pioneering piggyback denoting, a novel traceback increasing speed instrument for IP traceback. The primary thought is to abuse free ride open doors for facilitated and powerful conveyance of traceback message parts to endhosts. In light of this a trigger-based IP traceback approach, which underpins the traceback of individual parcels, Which at that point gave a hypothetical investigation of stamping based traceback, and demonstrated the capability of entrepreneurial piggyback checking. An adaptable stamping based traceback (FMBT) system, which meets a few great goals that past individual traceback plans neglected to fulfill at the same time. From [2] Inactive IP Traceback (PIT) which tracks spoofers dependent on way backscatter messages and open accessible data. We outline causes, gathering, and factual outcomes on way backscatter. We determined how to apply PIT when the topology and steering are both known, or the directing is obscure, or neither of them are known. We displayed two powerful calculations to apply PIT in huge scale arranges and sealed their accuracy. We exhibited the viability of PIT dependent on finding and reenactment. We demonstrated the caught areas of spoofers through applying PIT on the way backscatter dataset. The paper [3] an achievable DDoS assault source traceback plot, the checking on interest conspire, in light of the deterministic bundle stamping system. As a rule, the plan in a general sense tends to the versatility issue of the current DPM based traceback plans. Subsequently, we can traceback each assault source (switch) on the Internet, which is incomprehensible for the past traceback plans. The hypothetical investigation and certifiable informational collection based analyses exhibit that the proposed plan is possible. In respects of future work, the present work to improve the accessibility of the MOD server itself as it is an incorporated framework. Besides, the proposed plan to traceback to each every assault PC (however) by utilizing different bundles for stamping coding. Thirdly, a careful examination on the MOD framework is wanted, for example, the bogus positive rate and false negative rate of the MOD plan. At long last, a genuine framework model is intended to look at the effectiveness of the proposed plan by and by sooner rather than later. From [4] the absence of sending motivations, the best present enemy of mocking practices are deficiently sent on the Internet, and caricaturing assaults are as yet common. Another enemy of ridiculing technique MEF, which has the accompanying points of interest MEF furnishes ASes with high sending motivating forces for both d-DoS and s-DoS. Deployers of MEF can pick up a similar insurance as departure sifting, while non-deployers can't increase free assurance (on-request separating mode). MEF has no bogus positives when effectively worked. MEF brings about negligible organization cost. An AS just needs to introduce a product augmentation to NMS. The point by point structure of the MEF framework and a prefix pressure calculation to fit separating rules in switches' constrained asset. We assess the arrangement motivations of MEF in both hypothesis and reproductions with genuine Internet information and contrast it and existing enemy of ridiculing techniques. The outcomes demonstrate that the on-request separating method of MEF is the special case which accomplishes consistently developing sending motivating forces for both d-DoS and s-DoS. The execution and overhead of the prefix pressure calculation and the whole framework. From [5] A traceback display dependent on Autonomous System and Deterministic Packet Marking was proposed. The proposed strategy can follow the assailant till the entrance edge switch even with a solitary parcel which meets the fundamental necessity of system crime scene investigation. It requires ostensible handling and there is no capacity overhead. The main downside is the higher association of ISP working the AS. Future work includes execution examination utilizing reproductions to approve our method in correlation with the current traceback systems. Pleasing fracture of bundles, while utilizing the 32 bits utilized for discontinuity to check parcels, is additionally a test. The paper [6] it tells around an effective traffic source recognizable proof plan called Probabilistic Pipelined Packet Marking (PPPM) which intends to engender the IP locations of the switches that were associated with denoting certain bundle by stacking them into parcels setting off to a similar goal. Accordingly, protecting these addresses while keeping away from the requirement for long haul stockpiling at middle switches. Such plan is exceptionally valuable in recognizing Denial of Service (DoS) assault sources. The fundamental preferred standpoint of utilizing this method in PPPM, is to altogether diminish the quantity of parcels required by the unfortunate casualty in the traceback procedure, which prompts quicker and versatile distinguishing proof of assault sources.

3. Objective

The main objective of this paper is to find out hacker in an efficient and quick way with the person's location with his exact latitude and longitude and also the ISP of the intended person to find out , this way we can block the IP so that the person cannot further attack , by this way the system is more efficient .

3.1 Existing System

IP traceback is a compelling answer for distinguish the wellsprings of parcels just as the ways taken by the bundles. It is basically propelled by the need to follow back system gatecrashers or aggressors with ridiculed IP addresses, for attribution just as assault safeguard and moderation. For instance, traceback is valuable in shielding against Internet DDoS assaults. It likewise helps with alleviating assault impacts; DoS assaults, for example, can be relieved in the event that they are first distinguished, at that point followed back to their starting points, lastly obstructed at passage focuses. Moreover, IP traceback can be utilized for a wide scope of viable applications, including system crime scene investigation, security reviewing, organize blame analysis, execution testing, and way approval. In any case, it have its hindrance of abusing traceback to find ISP system of topology and furthermore have a downside of circulated logging which needs in favoring fractional organization.

Proposed System

We initially present a novel cloud-based traceback engineering, which misuses progressively accessible cloud frameworks for logging traffic digests, so as to actualize legal traceback. we likewise address the entrance control issue in the cloud-based traceback design. To this end, we propose a system for verification in cloud based IP traceback, named FACT, which upgrades customary confirmation conventions, for example, the secret key based plan in cloud-based traceback. Our key thought is to install fleeting (time sensitive) get to tokens in rush hour gridlock streams and afterward convey them to end-has in a productive way. The proposed technique not just guarantees that the client (or element) mentioning for traceback administration is a genuine beneficiary of the parcels to be followed, yet additionally adjusts well to the constrained checking space in IP header. Assessment thinks about utilizing certifiable Internet traffic datasets show the practicality and adequacy of our proposed FACT traceback confirmation plot.

3.1.1 System Architecture

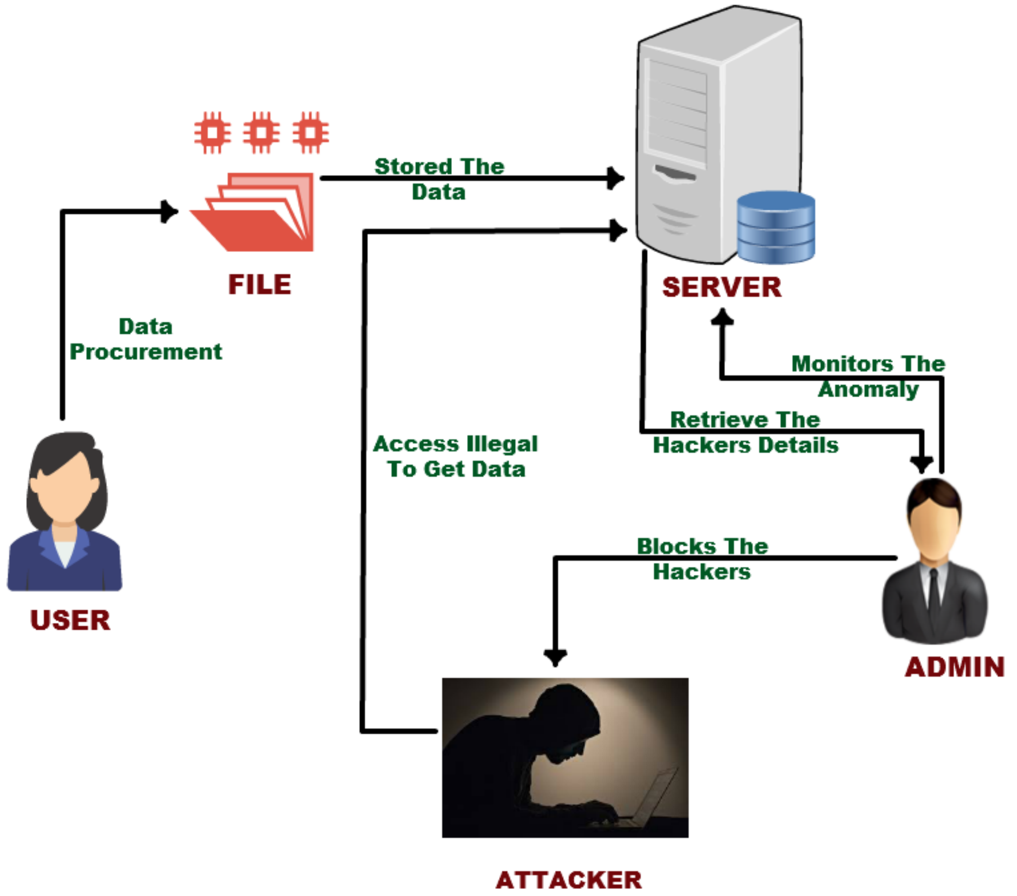


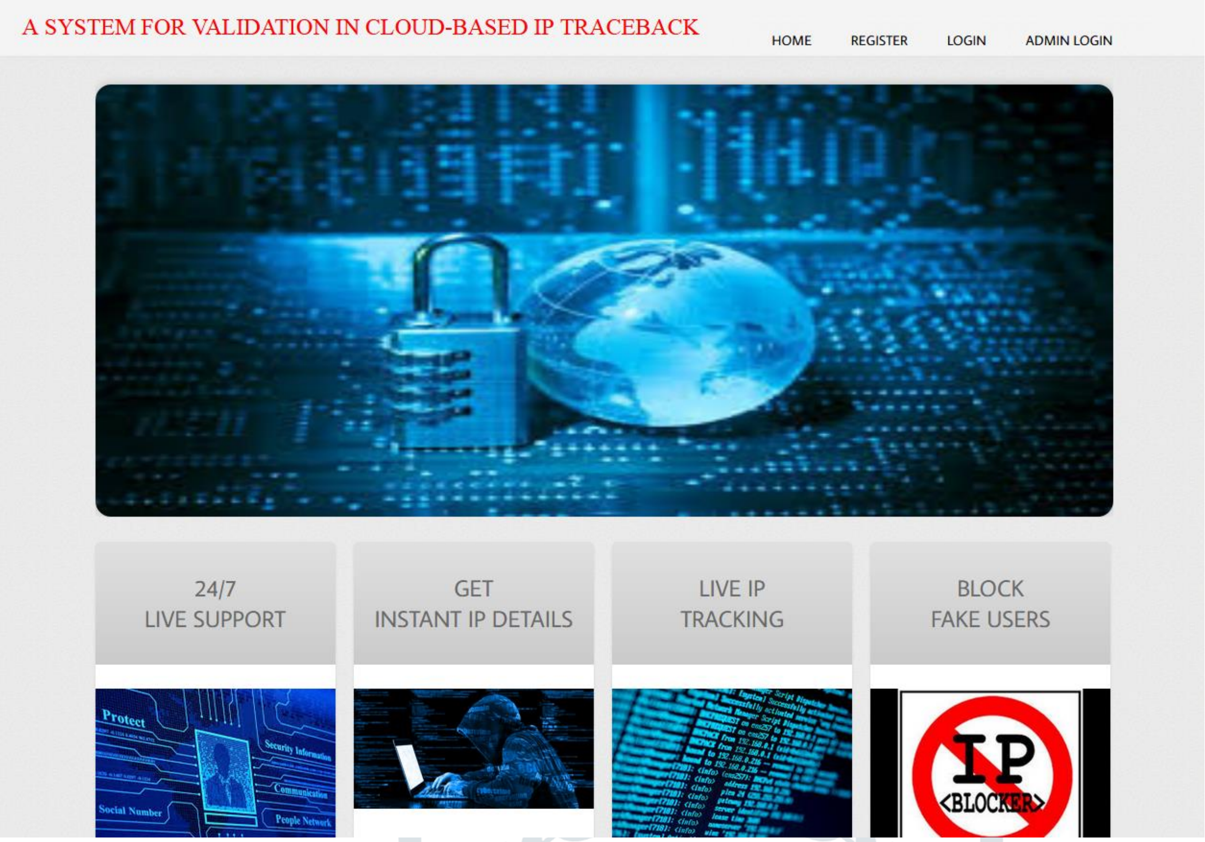
Fig 1 System architecture of proposed scheme

3.1.2 Functional Modules

- Network ID Creation and data upload
- Intruder check and Find IP ISP
- Get Intruder IP longitude & latitude and Get Access point & Gateway
- Block Unwanted User

Network ID Creation and data upload

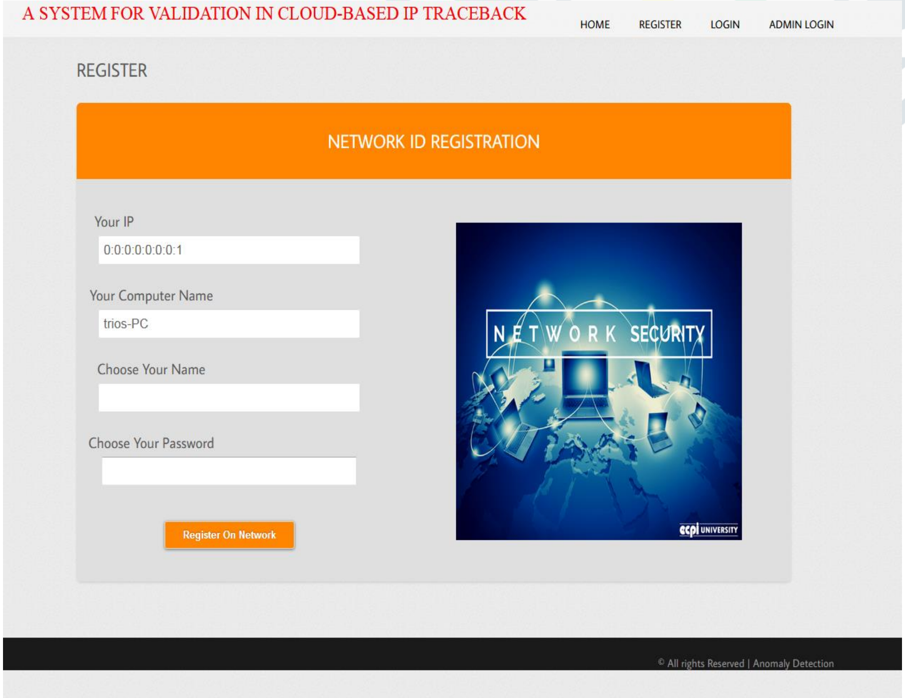
In Net ID Creation Everyone Should be register our Own Details like User Name And secret key, your PC IP address and MAC Address for login reason. In this venture consequently to get the scope and longitudes and send back the administrator. For every PC an default IP address will be available which will be registered even the person enters it incorrectly in order to trick the system. After registering the user should login and while the time of uploading file an cipher text is generated using random key generation after the generation of key it will be encrypted using AES which is a 16 bit encryption algorithm the random key generated will be used for other users while downloading which acts as a authentication system.



A SYSTEM FOR VALIDATION IN CLOUD-BASED IP TRACEBACK

Intruder check and Find IP ISP

Obviously as an hacker he will try to enter the fake credentials to enter the system , once the fake credentials are inserted , the page will be responding like other pages **" incorrect username or password"** but at the backend the person's IP address along with his ISP , his latitude and longitude will be reported back to admin so that he can be blocked by the admin. The IP address is found by "inert address protocol" .



A SYSTEM FOR VALIDATION IN CLOUD-BASED IP TRACEBACK

REGISTER

NETWORK ID REGISTRATION

Your IP
0:0:0:0:0:0:0:1

Your Computer Name
trios-PC

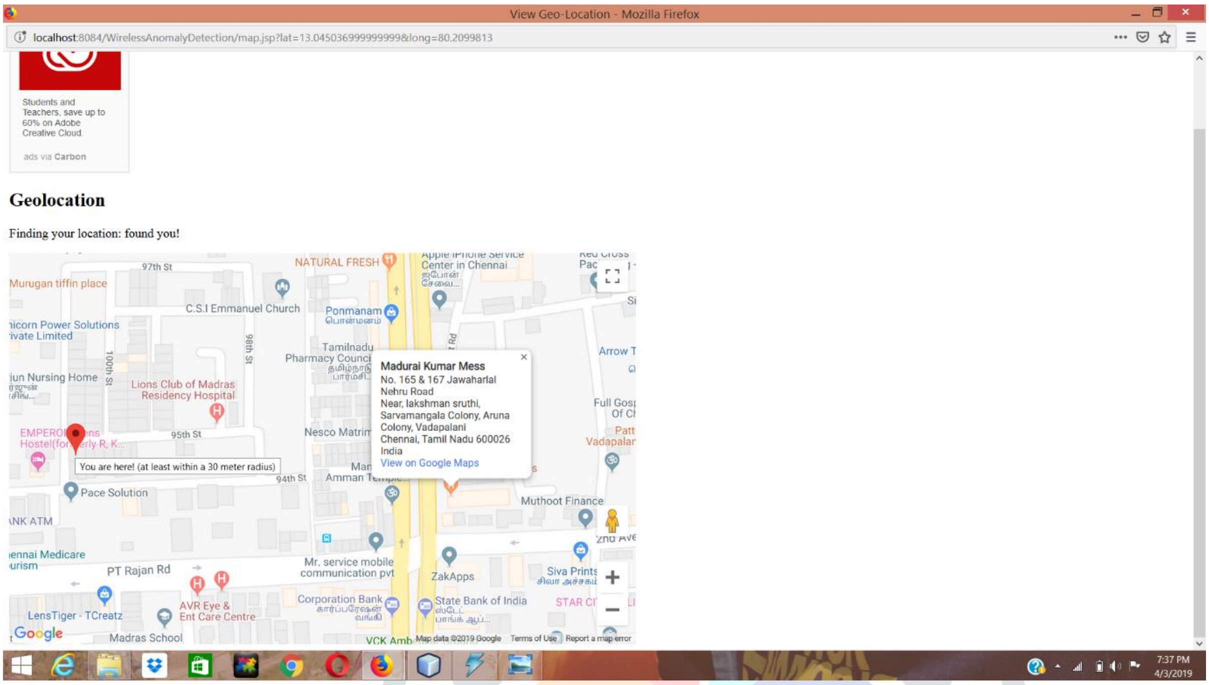
Choose Your Name

Choose Your Password

© All rights Reserved | Anomaly Detection

Get Intruder IP longitudes & latitudes and Get Access point &Gateway

The possibility of tracking out the person's location with his latitude and longitude can be done with the help of web components using IP address , and admin will be tracking the respective ISP of the intended person using jquery web service components , which leads to provide the location precisely. The attacker can be found in real live location using geo location , we can get the coordinates of latitude and longitude by using google api.



View Geo-Location - Mozilla Firefox

localhost:8084/WirelessAnomalyDetection/map.jsp?lat=13.045036999999998&long=80.2099813

Students and Teachers, save up to 60% on Adobe Creative Cloud.

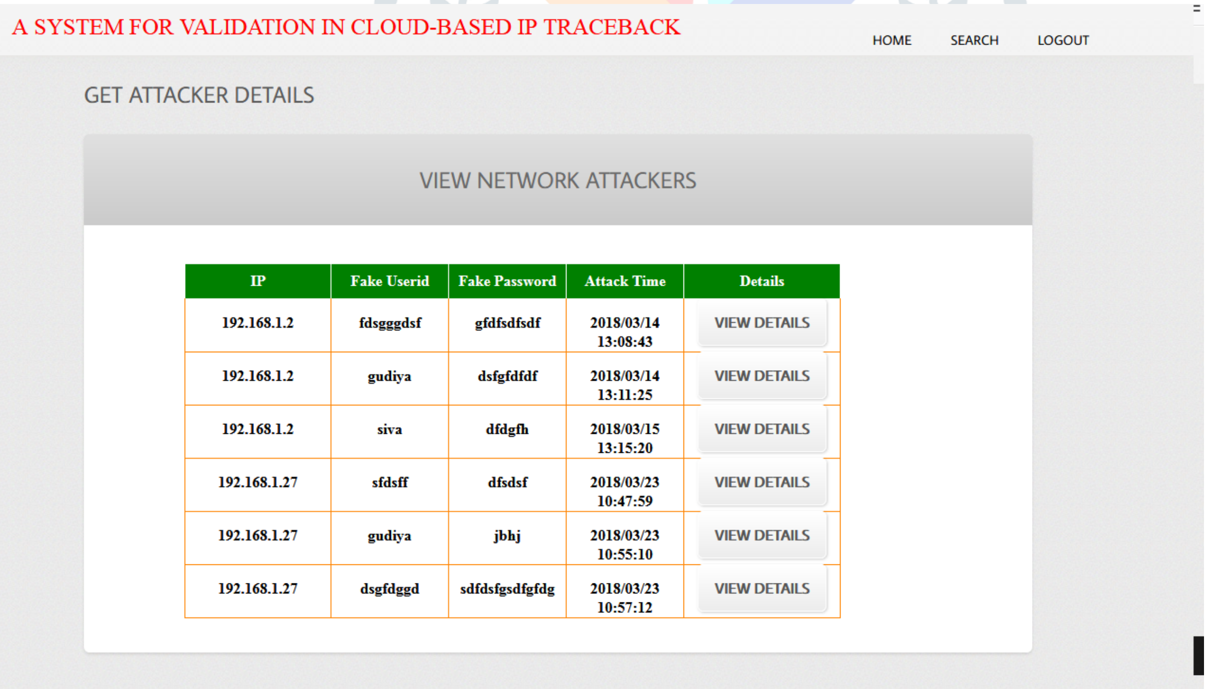
ads via Carbon

Geolocation

Finding your location: found you!

Madurai Kumar Mess
No. 165 & 167 Jawaharlal Nehru Road
Near, lakshman sruthi, Sarvamangala Colony, Aruna Colony, Vadapalani
Chennai, Tamil Nadu 600026
India
View on Google Maps

You are here! (at least within a 30 meter radius)

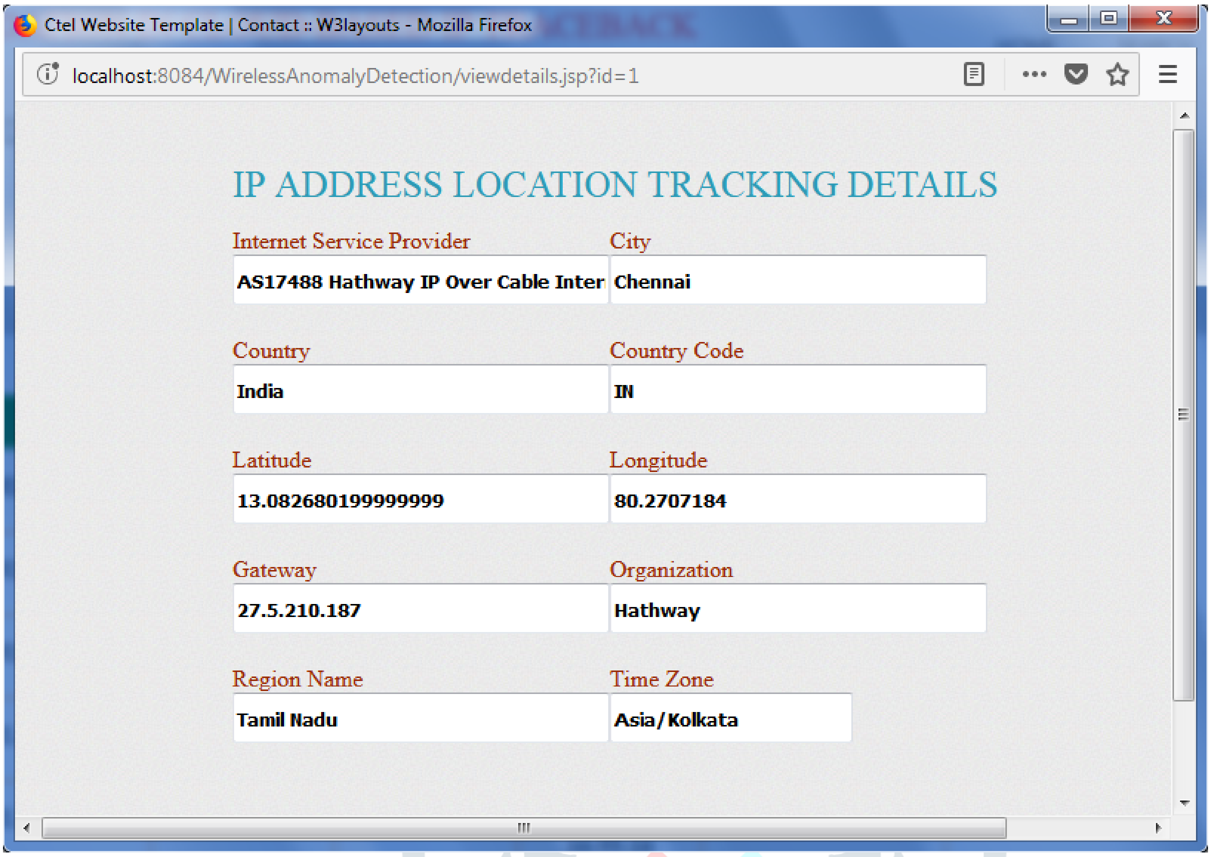


A SYSTEM FOR VALIDATION IN CLOUD-BASED IP TRACEBACK

GET ATTACKER DETAILS

VIEW NETWORK ATTACKERS

IP	Fake Userid	Fake Password	Attack Time	Details
192.168.1.2	fdsgggdsf	gfdfsdfsdf	2018/03/14 13:08:43	VIEW DETAILS
192.168.1.2	gudiya	dsfgfdfdf	2018/03/14 13:11:25	VIEW DETAILS
192.168.1.2	siva	dfdgfh	2018/03/15 13:15:20	VIEW DETAILS
192.168.1.27	sfdsff	dfsdsf	2018/03/23 10:47:59	VIEW DETAILS
192.168.1.27	gudiya	jbhj	2018/03/23 10:55:10	VIEW DETAILS
192.168.1.27	dsgfdggd	sdfdsfgsdfgfdg	2018/03/23 10:57:12	VIEW DETAILS


Ctel Website Template | Contact :: W3layouts - Mozilla Firefox
localhost:8084/WirelessAnomalyDetection/viewdetails.jsp?id=1

IP ADDRESS LOCATION TRACKING DETAILS

Internet Service Provider: AS17488 Hathway IP Over Cable Inter

City: Chennai

Country: India

Country Code: IN

Latitude: 13.082680199999999

Longitude: 80.2707184

Gateway: 27.5.210.187

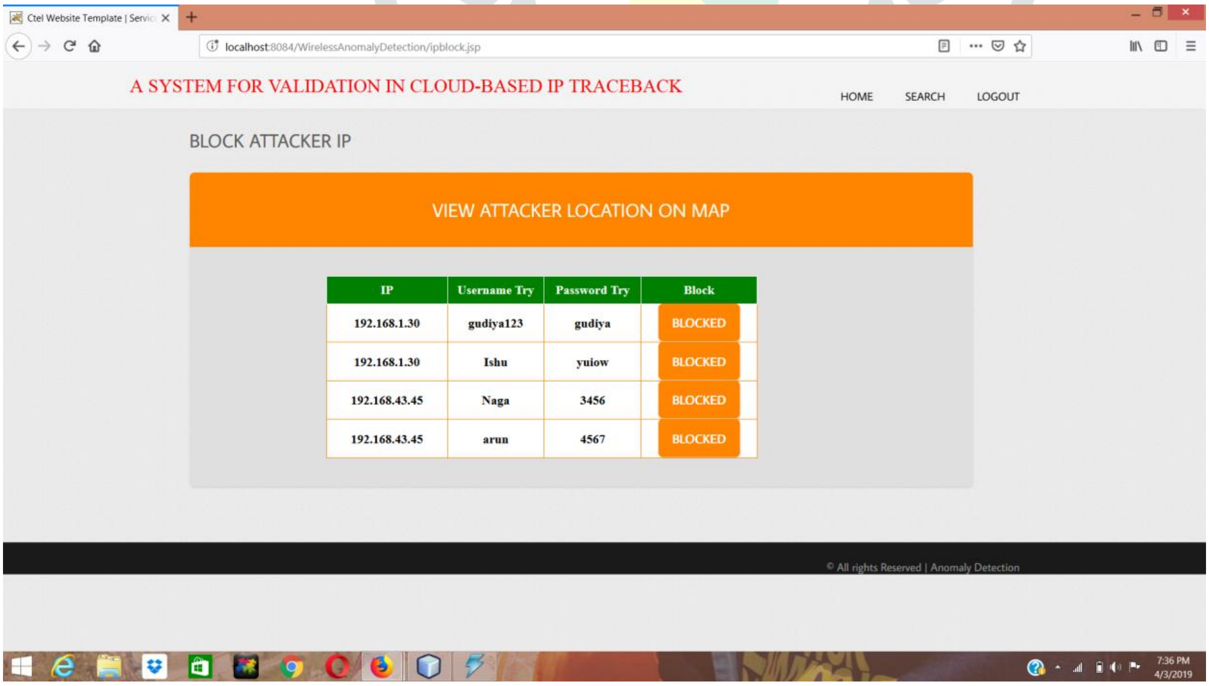
Organization: Hathway

Region Name: Tamil Nadu

Time Zone: Asia/Kolkata

Block Fake user:

After finding out the fake user the admin will be reporting him and he will be terminated immediately from accessing the website again. Once the address is found it can be easily trace out the location in google maps which is convenient for identifying the person.


Ctel Website Template | Servic
localhost:8084/WirelessAnomalyDetection/ipblock.jsp
HOME
SEARCH
LOGOUT
VIEW ATTACKER LOCATION ON MAP
© All rights Reserved | Anomaly Detection
7:36 PM
4/3/2019

A SYSTEM FOR VALIDATION IN CLOUD-BASED IP TRACEBACK

BLOCK ATTACKER IP

IP	Username Try	Password Try	Block
192.168.1.30	gudiya123	gudiya	BLOCKED
192.168.1.30	Ishu	yuiow	BLOCKED
192.168.43.45	Naga	3456	BLOCKED
192.168.43.45	arun	4567	BLOCKED

4. Conclusion

The network security activity we discussed in this paper have an more impact on sharing files as the hacker will be immediately will be get caught at the first chance ,even without knowing the backend process , we also create a random cipher text at the time of uploading file which should be known by the user who is going to download which will be requested to owner back so that system is more secured for file sharing and at the same time our main intention of tracing back to hacker's IP is successful using the implementation of FACT , Further we can improve the system by including the project at P2P network which will be more effective for using in blockchain process.

References

[1] Long Cheng, Dinil Mon Divakaran, Wee Yong Lim, Vrizlynn L. L. Thing," Opportunistic Piggyback Marking for IP Traceback", 2015 IEEE conference .

[2] Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE "Passive IP Traceback: Disclosing the Locations of IP Spoofers from Path Backscatter", IEEE Transactions on Information Forensics and Security

[3] Shui Yu, Senior Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Song Guo, Senior Member, IEEE,

and Minyi Guo y , Senior Member, IEEE," A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking" ,2015 IEEE .

[4] Bingyang Liu, Jun Bi, Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE, "Toward Incentivizing Anti-Spoofing Deployment", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 3, MARCH 2014.

[5] Emmanuel S. Pilli, R.C. Joshi, and Rajdeep Niyogi," An IP Traceback Model for Network Forensics"

, EUDL 2015.

[6] Basheer Al-Duwairi and G. Manimaran Dependable Computing & Networking Laboratory Dept. of Electrical and Computer Engineering Iowa State University, "A Novel Packet Marking Scheme for IP Traceback", Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04)