Trust Models Dos Attacks on E-Government Services

SLOT – F1

Submitted by:

Dodda Sumanth (18BCI0067)

Gogireddy Manohar (18BCI0077)

V Venkata Narendra (18BCE0515)

Abstract:

With the growth of internet and availability of internet, government services have also taken up an online path to serve the people better. E-government services provide greater efficiency than a normal office method, this way people can look up their info or process their query without waiting for much time at the office for the people over there to fetch their records.

With the growth of these services their security is also a major problem to be dealt with. Any server accessible to the public will be attacked at some point or the other by an attacker. there will be some people that misuse them or exploit these services that are present in cloud servers or standalone servers for their own benefits or just for fun. One of the most common attacks on services like these is Denial of service attack. In denial of service attack the attacker sends unwanted traffic towards the server or some command to make the system crash. Attacker abuses the systems so that other people can't access the resources present on these systems. To provide security to these systems we have thought about using a trust model that categorizes the users into trustable or not trustable.

A lot of Trust models have been published in the past years for various other use cases, we chose some features from them to fit our use case in the best way possible.

Introduction:

E-government services can be classified into 4 types:

Government to Citizen (G2C): Government sets up websites that citizens can access and quickly lookup their info and download various documents that they require in order to do some process or use it as an identification service. They can also get government information from these sites.

Government to Business (G2B): This is a non-commercial interaction between governments and businesses for sharing advices on best practices. This can also be used for sharing information about a business. This can also be used to view the legal actions that are active on the business or evaluation of books and contracts between the business and the government.

Government to government (G2G): Government to government is interaction between separate governing bodies of the same government. This is a collaborative environment for various sectors in the government to come together. These interactions can be between State government and central government or between state government and the commercial business sector of the government.

Government to Employees (G2E): This interaction allows employees to interact with the governing body immediately using some tools. G2E is an interactive way to bring together the employees of different sectors to knowledge. This G2E can also be used to give e-payrolls, e-benefits, e-training.

Trust definition: Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently or his capacity ever to be able to monitor it) and in a context in which it affects his own action.

Need for trust :The most important concern in the Internet world (i.e. e-Business and e-Government) is how to trust that we are buying from the right shop, we are paying the right person, we are dealing with the right entity, the items will arrive after we have paid for them, our privacy is preserved, our personal files and records are kept securely, our business process transactions are related professionally, and that there is nobody monitoring our credit card details or our login credentials. These are the issues the networking environment has to resolve before we put our faith in the Internet transactions system.

Trust concerns: Trust is a central defining aspect of many economic and social interactions. “Building trust is a core requirement for establishing new relationships concerning security, confidentiality, integrity, non-repudiation, trust, etc, especially in an online virtual environment.

Our trust model Works in G2C models and mainly focuses on Prevention of Denial of Service attacks on E-government systems using a trust model. Trustable users can access the system without any limitations that can prevent them from using the systems. The users that have lost their trust cannot access the system without a penalty being imposed on to them.

In the papers that we have taken references from authors have suggested various methods of establishing trust values, calculating them and restricting users from doing unwanted activities. We have also studied some methods to prevent DOS attacks, but DOS attacks can come in all forms ranging from traffic overloading to system crashing, software crashes, bug exploitations, abusing system firewall to make it ban some users. Various kinds of internal attacks and many more.

In our model we have thought about establishing trust tokens that carry some value within them and their authenticity checking to be done by an application and using a firewall to prevent basic level DOS attacks that fill up network bandwidth to prevent other users requests from reaching the system. A threshold will be defined for user trust and the value of trust lies within the range (0,1). If the value goes lower than the lower limit for the acceptable trust then the user will be denied from accessing the systems. That IP will be blocked at the firewall using iptables tool available on the Linux system.

The idea to use tokens has been inspired by the paper “A cloudlet-based security and trust model for e- government web services” and other models.

Motivation:

When we set out to research the usage of trust model in government to prevent security offences, we could only find 1 paper that was directly related to the topic at hand. This inspired

us even further to propose our own security framework. We have taken parts of existing research to be used in our framework. Trust models in combination with firewalls can prove to be more useful in case of a repetitive sophisticated attacks. Firewalls that are already present can mitigate easy attacks like flooding. So, a much complex system for mitigating complex attacks was needed for this specific use case.

Aim and Objective:

To develop a framework that can deal with Denial of service attacks by using a trust model so that normal harmless users aren't affected in any way during an attack and can carry out their work with the government services without any interruption.

Literature review:

Title: Security Engineering for E-Government Web Services: A Trust Model (18BCI0077)

Abstract: With the extensive usage of e-government web services in the current technological generation securing these services has become more demanding than ever because of all the attacks that happen on these services all the time. In this paper a security trust model has been introduced to secure the communication between governmental web services and is entrusted to a trusted third party to establish and maintain this for a government.

Web service security countermeasures:

W3C XML encryption: This algorithm can be used to encrypt or decrypt the SOAP messages between two web-services, but the soap messages encrypted using this method can be decrypted by an adversary in an easy way.

W3C XML signature: Each SOAP message sent by any service must have a signature of the sender to provide non-repudiation and integrity.

WS-Security Tokens: SOAP messages can be used by an attacker to compromise the communication between the web services. WS security tokens can be used by the receiver to identify and verify the sender's identity. These tokens can be used to convey information within a SOAP message and they are defined in the XML of SOAP message. Some extensions to the WS-security to improve its security in the works like "M. B. Brahim, T. Chaari, M. B. Jemaa, and M. Jmaiel. Semantic matching of WS-security policy assertions."

WS-secure conversation: it is used to determine a way to create a security context recognized by an URI. that will authorize the existing SSL/TLS connection to be utilized by subsequent requests to a web server at the transport level. This provides a basic mechanism on top of which other mechanisms for secure messaging can be implemented for multiple message exchanges.

WS-policy: This model can be used to set policies to a web server to specify requirements, capabilities and properties of a web-service. When a request is sent these policies are used to

validate and accept the request. These policies can be defined at service endpoints or can be specified in the XML data. These policies can be retrieved from SOAP messages using WS-metadata exchange.

WS-trust: This protocol was designed to ease the Web-services interaction by using SOAP messages in a common trusted way. This protocol depends on exchange of secure trusted tokens.

These tokens are sent to a web-service attached to a SOAP message to gain access to the services provided by that web-service.

XACML: extensible Access control markup language is an approach for making secure communication viable in web-services by defining an XML framework for exchanging authentication and authorization tokens or details.

Methodology:

This third party involved with the government is responsible for the security of communication between the government services as well. They give a valid identity to a service for the purpose of communication. The identity of this service can be encrypted using XML encryption techniques before transmitting this identity through Simple Object Access Protocol (SOAP) to another service. This identity sent through SOAP is used to validate the identity of each service through a third party before participating in any action. This way we can provide an assurance of integrity and non-repudiation of the transmitted SOAP message. The communication between third party and web services is also controlled by the third party using a PKI technique. The third party is responsible for publishing the public keys required for communication in this protocol and it is required to publish the public keys using its private key.

Title: E-Government and Cloud: Security Implementation for Services (18BCI0077)

Abstract and introduction: To make the government services easily accessible to the population e-government services have been implemented. They have ensured greater efficiency, transparency and operability. But with this comes the challenge of security and trust. This paper will discuss a security framework that will facilitate both authentication and authorization for Web services offered public administration services deployed in the cloud. This framework implements existing methods for security in the cloud and has added some proprietary methods to ensure that they fit in together. This framework has been proposed with the idea of unifying all the e-government web services under a single authentication and authorization model.

Methodology: In this paper the author has used The Public Digital Identity System (Sistema Pubblico d'Identità Digitale - SPID), The Security infrastructure defined by the Agency for Digital Italy.

SPID and The Security Framework: SPID has three different types of authentication methods.

1. Username and password
2. Username and an automatically generated temporary password
3. Username, password and an access device.

This model allows users to access the services with different privilege models and choose one according to their instantaneous needs. The framework proposed in this paper acts as an intermediary between the Identity providers and service providers.

A federation model can be used to make all the e-government services offered by different governing bodies to be accessible under a single login.

Web applications and service integration: Integration of web-services can be done by using an authentication module that uses OAuth2/OpenID connect or some other open and widespread tools. The author has also explained how OAuth works for the customer to be able to access the services without putting in 2 or more usernames and passwords.

Policy Agent: Policy agent is a component that's installed on the server hosting the web-service. Policy agent's duty is to intercept all the requests being sent to the resources available on the server and verify the authentication and authorization of those requests. After the user has been recognized they are sent to the resources that they have requested.

Reverse Proxy: Reverse proxy is a software that resides between the internet and the server. Reverse proxy is a standalone server that has been placed with solely the purpose of protecting the main server from attacks. This is used in cases where a policy agent is not suitable to be used.

The order in which these events occur are:

- User requests the service
- DNS returns the address of the reverse proxy server
- Request is intercepted by the reverse proxy or policy agent
- If the policy agent doesn't find any valid tokens for the user then a new token is generated by authenticating and authorizing the user.
- Policy agent verifies the user session, adds user data and forwards it to the resource manager by modifying it to make it understandable to the resource manager.
- Resource manager processes the request and sends a response through the reverse proxy.
- In case of any malicious activity from a user or IP address it can be blocked by the policy agent on the reverse proxy server.

Title: A trust model based on theory of evidence for E-commerce environment (18BCI0077)

Methodology:

In this paper a new trust model has been proposed based on trust scale and theory of evidence. This model can depict the trust evaluation and merge the computed result based on different trust scales. In this model Dempster-Shafer theory has been used. This model has 3 levels of trust for a peer. It can be either good or neutral or bad. But the trust can exist between these states like a peer might not be able to decide between good or neutral. The peer can even be uncertain regarding a peer. The sum of all levels of trust when put in a function should be equal to 1. uncertainty means that the overall value of the function m is exactly equal to 1 because any other attribute doesn't have any value. If the user gets any evidence his trust might change and the value of some other attribute can be determined, so the value of uncertainty becomes less than 1.

One of the important steps in this trust model is to acquire trust.

Trust Scale: Trust evaluation system gives feedback about other peers who they have to interact with. We define the trust with a word rather than using a number so that the users can understand what they're looking at

Trust acquisition: A peer can have different parameters to rate their trust like quality of service, speed of service. In order to obtain the trust value of a peer we have to aggregate the values of trust of all parameters to form a comprehensive trust value. Computational approximation used to obtain a unified value of trust in case of 2 peers is $m(A) = \underset{A \subseteq B}{} m(B)/\Sigma m(C)|C|$. And 0 for others. The peers' comprehensive value can be obtained by adding all trust values. This follows the principle that when two evaluations have the same tendency then their aggregation also has the same tendency.

The decision making is directly proportional to the value of good review and inversely proportional to the value of rating of bad review. When the review is neutral then it is considered as positive. A very good trust value based on reviews can be lost very quickly from the negative rating. When the overall trust falls below 0 the user will be blacklisted.

Title: A Collaborative Trust Model of Firewall-through based on Cloud Computing (18BCI0077)

Methodology:

This trust model firewall is based on the domain trust model which divides cloud into different domains and trust between domains are divided into within domain, inter-domain, outside domain relationships. A trust table updates the trust value of nodes which have traded with other nodes within the domain. Each domain has three tables DITT (domain inside trust table) DOTT (domain outside trust table) RVT (risk value table). DITT stores the trust values of nodes in the domain. DOTT is the average of trusts of the nodes in other domains. RVT can be calculated using the definition of risk. When a node requests a value the domain queries other domains and uses its own trust table to find out the overall trust of that node and carries out the request

depending on the trust values of that domain. If the transaction is being carried out for the first time then the requester has to send its digital signature to establish a value of trust with the domain.

Since the trust can change with time a decay function has been proposed to decrease the value of trust overtime. This model has employed a basic decay function that calculates the overall trust from the trust value that has been stored in the trust table a long time ago. The function is as follows: $T(t) = 1/(1+ \lambda*(\text{current time - previous transaction time}))$. Where λ is a constant with a value of 1/604800.

Trust value is updated every time a transaction occurs depending on the success or failure of that transaction. A special function is used to calculate the updates in trust value. When the transaction succeeds the value is increased and when the transaction fails the value of trust will be decreased. If there has been no transaction history between these nodes then the value of trust will be obtained from the DITT if the node lies in the same domain and the time function will be applied to it. If the node exists outside the domain then the trust value will be obtained from the domain in which this node lies and then the trust is calculated. Whenever a transaction is successful update TT DITT and DOTT.

Title: Study on Double-Layers Trust System and Model of Trust in P2PEB mode (18BCI0077)

Methodology:

Double layer trust mechanism consists of 2 types of mechanisms. Direct trust and indirect trust.

Direct trust: Direct trust can be used when the two trading parties have interacted in a trade with each other before.

Indirect trust: Indirect trust is when one doesn't know the other party at all and hasn't had any interaction with them. In this situation one goes to a trusted third party to establish some trust about the other party.

In peer to peer e-business mode, enterprises are individuals rather than a big company. The trust gained from trade experiences by these enterprises is fully trusted. Whereas the trust obtained from another enterprise or party is not trustable. In order to make this trust work two trust mechanisms have to be used.

Trust model:

Consider two parties i,j that have traded for n times. Let t_k denote the time at which the k^{th} trade was done. Direct credibility: The trust obtained by the enterprise by trading with the same enterprise previously. Indirect credibility: The trust obtained from a third party. This value changes from time to time and is in between 0(absolute distrust) and 1(fully trusted). Trade

evaluation: This is the measure of satisfaction with the trade. When the evaluation value is less than a set value it is said to be a malicious trade.

Calculation of direct credibility: Direct credibility is directly proportional to the trade evaluation value and inversely proportional to the time between the last trade and now. When the trade evaluation value is less than the threshold set by the company the value of direct credibility is set to zero. To do this a value has been defined that is multiplied to the sum of the trust evaluations.

Calculation of credibility: If a trade has happened between the two parties previously but not before long time the direct credibility is considered as the credibility, but if a long time has passed between the previous trade and the current one or if this is the first trade that has happened between these two parties then credibility is obtained from indirect credibility. If the trade has occurred within a considerable amount of time but it is nearing the threshold then a balance of Direct credibility and indirect credibility.

Title: Trust based secure routing mechanisms wireless sensor networks: A survey (18BCI0067)

Introduction:

Internet is growing day by day and the core of it the network. The source and the destination communicate with each other irrespective of their locations and without compromising with the quality of the content they send over the network. But the content while it travels through the internet should be secured so we have 4 levels of security to be provided they are end system level security, end-to-end security, QoS level security and securing the infrastructure of the deployed network. So, Wireless sensor Network (WSN) is a technology used by the applications that deal with confidential and sensitive data.

Methodology:

WSN usually works using a wireless medium and is ad hoc in nature. So, for the transfer of the data a particular node might night rely on the neighboring node and the nodes must always be in a centralized administration in order to transfer the packets between the nodes. The topology dynamically changes when a node adds to the network or when a node leaves the network. There is always a chance for WSN to offer both routing mechanisms and security resiliency. So, secure routing becomes inevitable for WSN.

It is essential for WSN to get rid of certain threats and attacks, and in addition it has to ensure authentication, confidentiality, integrity and QoS. WSN is generally attackable to some attacks like Modification attacks, replay attacks, Black hole attacks, Gray hole attacks, Jelly attacks, flooding attacks, Rushing attacks, Wormhole attacks, Sybil attacks and Collusion attacks.

The fundamental unit in data network is data. So, the fundamental task of WSN is to include data capturing processing and transferring the data from one node to the other node. The data trust models might prone to bad mouthing attacks. Here are few data trust models to be considered: RFSN which is used to control the ineffective mouthing threat by sending the good reputation information. Trust and Energy aware Routing Protocol (TERP) computes the trust values by

exchanging data with its neighbor nodes. Determining Faulty Readings (DFR) is used to identify the faulty readings that are either intentional or unintentional.

There are two types of node trusts, Centralized node trust model and Distributed node trust model. Here are various node trust models available, Trust Computation mechanism (TCFL) is used to select the trusted pathway from the sources. RFSN is used for maintaining consistency of the network. Parameterized and Localized trust (PLUS) is used for computing the trust regarding the accessibility of the sensor hub and the number of packets sent. There are other trust models for cluster based WSN like GTMS, TMBBT and HTWC.

Conclusion:

Trust model has a powerful mechanism to detect harmful nodes and their behavior. Once a node is detected as malicious node the neighboring nodes can use this trust information and stay away from this malicious node. So, improving the security features can lessen the security attacks and thereby deliver great performance.

Title: An Integrated Trust Model for Business-to-Consumer (B2C) E-Commerce (18BCI0067)

Introduction:

Majorly there are two types of websites, e-commerce websites and e-information websites. The main goal of the e-commerce websites is to give their customers the confidence that their transactions are secured. So, trust is considered as a key factor for all such transaction related websites. The concept of trust includes many disciplines like philosophy, sociology, economic organization theory and technology. Several other factors which might add up to the customer safety and trust are being added and integrated by the security measures.

Now-a-days there are many E-commerce organizations running in the society. But many of them failed to reach their potential destinations due to lack of trust as the day to day the transactions on internet are increasing from day to day life, we have been moving from the shops like retail shops to the cloud environment or hosting or managing a website online on their own.

Methodology:

The concept of trust is fuzzy and dynamic. The fuzzy nature indicates that the nature of the trust is imprecise and cannot be explained easily. Moreover, the value or the measure for trust is not constant and keeps changing. The extent to which a customer feels confident about a trustee is mainly dependent on the dimensions like integrity, benevolence and ability of the trustee.

The risks that customer might face can be classified into technology related risks that are derived from web-based technology and business-related risks like misuse of the customer related information and problem in the transactions. The multidimensional trust in electric commerce include four high level constructs like disposition to trust, institution-based trust, trusting beliefs, and trusting intentions.

Model of trust in Electonic commerce(MoTEC) has a main objective to access the trust worthiness of an e-commerce vendor and how the trust is established between a seller and a

consumer. The conceptual high-level model for a trust management evaluates the worthiness of a trustor and trustee based on the trustor goals. Technology Acceptance Model (TAM) is being widely used for studying online transactions. The extension of the TAM model with salient belief about the privacy and security should be considered by the users who deal more with online transactions and decisions to accept or reject the online environment.

The main constructs in the TAM model are explanatory variables like security, privacy and web page content. Moreover, the features of the websites play an important role in persuading the customers to do an online transaction. For a vendor to be a trustee for a customer, he needs to gain the integrity and benevolence. the customer will also be able to know the level of satisfaction from the previous customers of a particular vendor before they do an online transaction.

Conclusion:

TAM model is expanded by including important constraints that may reflect the trust between the costumer and the vendor through an online-transaction service and the present world is moving more towards the e commerce website this is the future so that it has to maintained and developed accordingly

Title: A Fuzzy Trust Model for E-Commerce (18BCI0067)

Introduction:

Now-a-days there are many E-commerce organizations running in the society. But many of them failed to reach their potential destinations due to lack of trust. This trust evaluation can be done based on extracted information by using fuzzy logic method. This method considers various factors like uncertainties with in E-commerce data, human relationships which makes this method best suitable for trust evaluation. In this method rather than expressing trust in numerical values it is expressed by linguistic terms. We now consider two models to see how trust evaluation is done.

Methodology:

In our trust model, we are mainly concerned from customer’s point of view and with that information we help them to decide whether to make in a transaction or not with their vendors website. As there are many unknown cyber merchants, this model just identified four major factors which need to be looked before dealing with merchants who are unknown. The four major factors are: Existence, Affiliation, Policy and Fulfilment.

The important factor in building trust in customers is to establish the existence of merchants with whom they want to make a transaction. In order to satisfy merchants existence factor there are certain things that the customer needs to collect, this information includes the merchant’s Telephone Number, Fax and Address; mandatory registration and peoples’ existence. And the second factor Affiliation looks at endorsement made by third party. The third factor Policy will completely look at information like privacy statement, customer satisfaction policy and warranty police. And finally, the fulfilment factor completely depends on methods and modes of payments, delivery methods and the community comments.

In Fuzzy Inference System there are two main concepts that deals with our application purposes. The first concept is a Linguistic variable and the second is that of a fuzzy IF-THEN rule. The linguistic variable is a variable whose words or sentences are completely in synthetic or natural language. And in IF-THEN rule it contains linguistic variables in the antecedent and the consequent parts. We use these two concepts in the fuzzy logic controller paradigm.

Due to the uncertainties involved it is hard to assess the trust relationships among customers and vendors. We have two main advantages of using fuzzy-logic to evaluate trust in E-commerce applications. This fuzzy type of method is capable to evaluate uncertainty in measuring the trust index among the vendors and also capable of evaluating imprecise data. And the second advantage of using this fuzzy type of method is it does decouple dependable variables while dealing with the variable dependencies in the system. As said, there are four modules which are used to measure trust now the fifth factor will be the final decision maker. The trust measure is calculated by considering three factors i.e., Pb is the risk that the consumer takes for trusting the E-commerce merchants, Lb is the loss the consumer has to bear when the transaction does not produce the result as expected and Gb is the gain entering the E-commerce transaction. It is calculated by using formula Gb=Pb-Lb.

Conclusion:

This fuzzy logic system supports to evaluating and quantification of trust in E-commerce. With the help of this system we are able to address many issues that other systems are unable to. So, in any E-commerce application trust measure plays an important role and that should be established by the merchant without any fail.

Title: Beyond “web of trust”: Enabling P2P E-commerce (18BCI0067)

Introduction:

As it is known eBay's are successful and can provide security to a certain extent. In this paper we speak about the vulnerabilities of centralized systems. So, in order to achieve security, we need to use authentication methods. One such service is PKI (public key infrastructure), but these are centralized architectures and contradicts the P2P approach. So, in order to avoid centralization again we use PGP applications like “web of trust". There are several doubts using P2P platform for trading highly valued goods, on the other hand C2C platform has equal risks like P2P.Initially by P2P public key infrastructure (PKI).

Methodology:

Essentially there are two dimensions in decentralized PKI management, namely “the discovery of peers who have the public key” and “trust on the peers from whom the public key by the authority

In web of trust, if person A trusts a person B’s key KB which is the public key of B, the person A also depends on B to certify or trust others. Here the strength of chain is estimated by the weakest link. A small vulnerability can cause a high damage. Statistical (quorum based) approaches, in this approach we gather public keys from many and maintain as a set and select

randomly. Hybrid, Combination of WoT and PQ approach – Hybrid PGP approach is inefficient (finding random paths) and insecure (intersecting paths)

P-grid properties Scalable, distributed search tree: distributed hash table (DHT), Randomized algorithms, purely local decisions, Efficient search and load balancing, Robust through massive replication, Support for updates, Support for identification, Semantic integration, Java implementation applications of p-grid, Trust assessment of peers, Peer commerce, Scalable, semantic Internet search, Decentralized public key infrastructure.

Bootstrap phase – Peer generates UUID (Puuid), public/private key – Insert tuple (Puuid, public key, IP-address, timestamp, signature) into P-Grid at Rmin1random peers so that Rmin2 distinct replicas receive insert – All replicas initiate updates – Update registered only if quorum of Rmin3formed – Puuid waits for confirmation from Rmin3 distinct replicas.

Operation phase – Routing of queries includes authentication of peers before forwarding requests using a challenge/response scheme and the stored public keys – Requestor collects all answers received from replicas and trusts the result if it can form a quorum of Rmin3 distinct replicas – Optimization, Peers store the public keys they learn about. Rmin1, Rmin2, Rmin3, are design parameters and can be defined individually by any peer-individual level of security.

Conclusion:

PKIs are key to support any form of e-commerce, C2C e-commerce is inherently decentralized- decentralized PKIs, Decentralized PKIs can offer similar QoS as centralized QoS but require no additional infrastructure and overcome the problem of a single point of failure, our decentralized PKI can provide probabilistic guarantees and works fine in a predominantly well-behaving environment.

Title: TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs (18BCI0067)

Introduction:

Vehicular Ad Hoc Networks (VANETs) are a subclass of MANETs that are main Cooperative Intelligent Transportation Systems for ensuring traffic security. Nodes co-operate by haring the information regarding the road conditions either by vehicle-to-vehicle and vehicle-to-infrastructure communications.

The VANETs trust-based approaches are classified into three types: entity-oriented, data-oriented and hybrid-oriented. The entity-oriented categories help in the elimination of dishonest nodes from the network. The data-oriented category assumes the data quality to secure the communication. The hybrid-oriented categories help in ensuring a secured connection between the nodes.

Methodology:

The framework design has Neighboring Evaluation module, Decision Module, Communications Interface, Message Classifier, Delayed Verification module and Intrusion Detection Module. The Neighboring Evaluation Module is responsible for computing the stability between the nodes, managing new nodes in the communication range and combing the trust and link stability to generate companion lists. Link stability sub-module checks if the

neighbor nodes are moving in the same direction and roughly with the same velocity. Messages classifier module checks the message quality by dividing the traffic into classes.

The core of the framework is Decision module which allows the combining of module weights in order to evaluate the received messages and revoke the dishonest nodes. The algorithm to find the dishonest node actually calculates the trust value, if the trust value of a particular nodes is less than the thrust to send value then that particular node is considered as a dishonest node. The algorithm always maintains a global blacklist, a local backlist and a gray list. So, after getting a particular node the algorithm first checks if that node is present in any of the blacklist and only after checking it starts the calculation of the trust value.

The decision process selects an appropriate node to send the message preferable among the trustable neighbors. The forward node is expected to be the most trusted stable and should be closer to the destination. Trust Global, TrustDVM, TrustRL, TrustIDM are used to compare the versions of a framework with another. The Time convergence of DDos attacks detection and Bandwidth usage under DDoS attacks are mainly used to evaluate a framework's performance against a DDoS attack.

Conclusion:

The framework is designed to establish an efficient trust in VANETs to improve the relation among the nodes through a delayed verification of exchanged messages. This helps every node to have a view abouts its neighbor node's behavior and it can even detect the DoS and DDoS attacks easily.

6.**Title: A Cloudlet based security and trust model for e-government web services** (18BCI0067)

Introduction:

Cloud Computing and Web services are the backbone of many applications because of their interoperability and accessibility nature. The web services can be published in the cloud environment using the web Service Description Language (WSDL). This language is expressed using XML in order to perform input and output operations. The Universal Description Discovery and Integration Standard (UDDI) explains the publishing of web servers in the cloud. Cloudlet is used to secure the message between the governmental web services and other web services. The cloudlet is used as a trusted third party that provides an identity for communication between servers.

Methodology:

The web service provider offers functionality in a standard format which is available in central service registry or Cloud. The web service consumer retrieves the data from the registry and use the description in order to connect with the web service. The scheme uses keywords like publish, bind and find.

The general security threats that might affect the web service are message assertion, where the attacker might modify the SOAP messages that originated either from the provider or the consumer. The other attacks include Loss of Confidentiality, man in the middle attack, Replay of message parts and Denial of service attacks. The security countermeasures include

W3C XML Encryption, W3C XML signature, WS-Security Tokens, and WS-Secure Conversations.

Cloudlet consists of some trusted datacenters that are connected to internet, with a goal to bring the capabilities of cloud more rapidly. The cloudlet security framework can handle the process like authentication, authorization, accounting and auditing. The cloud model computes the trust relation in order to rationalize and express the uncertainty of trust from the perspective of the consumer. This uses heuristics to compute trust for each and every agent.

The security trust model is based on the existence of the cloudlet. The proposed model works as follows; A consumer first initializes the request. The request is appended to data storage which is managed by cloudlet which is a third party having the digital signature. The web server of cloudlet verifies the consumer's request and then processes the connection to data storage of the cloudlet. So, when the connection is passed the identity of the producer is said to be verified and the data is appended to consumer file and the e-government file in the data storage. When a webserver processes a connection, a secure connection is established between the consumer and the consumer. When the web service consumer provides a feedback regarding the service of the provider it is stored as a score in the Cloudlet of that provider.

Conclusion:

The services that are migrated to the cloud due to the accessibility and interoperability nature are still having their concern towards security and trust issues. So, the connection between the consumer and the provider should be done in a more secure and trusted manner.

A P2P-based Trust Model for E-Commerce (18BCI0067)

Now-a-days there are many E-commerce organizations running in the society. But many of them failed to reach their potential destinations due to lack of trust as the day to day the transactions on internet are increasing from day to day life, we have been moving from the shops like retail shops to the cloud environment or hosting or managing a website online on their own. people now in the present world are mostly depending on the e-commerce websites and most of the time the major question for them is it secure and there has to mutual understanding between the user and the merchant so that the user can buy the products safely by paying online and the seller can receive his money safely when some brought something from his website.

So for this there has to some trust worthy management or a system to manage things safely for this to reduce the risk factor everyone will follow a trust model to incorporate with in and basically there are 2 types of trust based models one is central model where the every entity in this model will have the same as every entity they will be having a common central trust point and another type of model is transitive model where the recommendation is taken into consideration for trust worthiness as the wrong and negative recommendations leads to discover and make it to grow the most powerful and trust worthy

There are many models and ideas proposed regarding trust models for e commerce and there are many drawbacks to it some of them are in P2P trust model the value of the information and transaction are ignored and in traditional methods they will take long time to adapt and learn to become the best there are many type of transactions and our paper mainly focus on B2B and

P2P transactions and for this we taken some concepts into consideration and they are feedback for the model although its slow it takes time but bad model will be can be dropped faster and when the peer will be having threshold value based on that we will consider the feedback of the customer the calculations for the trust model will include many factors say recommendations feedback weighing accordingly.

In this trust model we have 3 steps to obtain and good P2P model they are

1. Cal. Direct reputation

2.Assessing recommendation factor

3. Determining global reputation

1.Calculation of Direct reputation factor:

This factor is generated based on the Peer's satisfaction degree, peers reputation and the the previous threshold value on the the peer and we can also set a certain interval for this to consider the value within the period if we make any changes in certain period so that we can see the reputation factor change clearly regarding that change and transaction value of the user will also be considered.

2. Assessing the recommendation factor:

And based on this factor leads to generate a global reputation value by considering local trust score and aggregation weight and threshold level of the user to get a legit value of the recommendation factor the system will be considering the feedback aggregation wait of the peers based above level of good threshold value fixed and the output data will be appended to 2 tables accordingly say transaction record table and local score table where the transaction record table stores and maintains the transaction records of the peers accordingly and the local trust table stores the global reputation aggregation of the each pair.

3.Determining Global Reputation:

By considering the direct reputation from certain period say u to v and the recommendation reputation of u to v by an equation with help of lambda which reflects the quotiety of direct reputation and recommended reputation.

Conclusion:

In this paper we a new methodology to solve and mitigate the risk factors involved in the e-commerce as the present world requires fast performance with security this can be a part of it to provide it.

Title: DDOS Attack Detection and Mitigation Technique Based on Http Count and Verification Using CAPTCHA (18BCI0067)

Introduction:

DDoS is a type of attack where the hacker sends huge data using different nodes from all over the world to the routers of the company/organization and making it to hang or crash because the

routers will not be able to handle a load of data that they are receiving from the hacker from around the world.

DDOS attacks are one of the most popular attacks all over the world the mechanism involved makes the server or the corresponding routers shut by making the service/website unavailable due to this many financial losses occurred to the companies and organizations it became one of the cyber threats to the many of the e-commerce and web-based applications so it needs to be detected and prevented

These attacks are done by the botnets which are being controlled by the hackers and they will interrupt the users to get services by consuming the resources available to them. And because of the open IP feature any user from all over the world can send the request and one of the drawbacks is that hackers can use botnets to send large amounts of data and these botnets are prevented and needed to be controlled using techniques and algorithms to make the server free from such attacks.

Methodology Proposed:

Here in this paper, they proposed three major steps to prevent and mitigate attacks they are:

A. Restriction of access
B. B. Limitation of rate and CAPTCHA.

Restriction of Access:

Here the concept involved is in here IP blacklisting where the access to that IPS get restricted whose access is denied those IP will get updated in the blacklisted IP table and simultaneously updated in every node of the network and the file termed as bad host file and the proposed an algorithm to detect and updating IP's wherein

Step 1 they will set a user policy and that needed to be accepted by the sender

Step 2 the routers will monitor all the traffic that goes through all over the network

Step 3: and similarly, all ports are monitored accordingly

Step 4 the router uses the default server IP and port to accept requests from the users

Step 5 the packet will be forwarded according to the route assigned

Step 6 the IP will go under the search of blacklisted IP

Step 7 if present the packet will be dropped there itself and proceeds

Step 8 if any action is detected the Ip gets added to the blacklisted file

Step 9 it flushes all the IP tables and updates new IP block list IP and this process repeats

B. Limitation of rate and CAPTCHA:

Here if the upcoming connection requests the same object with the same IP the router has to restrict its HTTP request by defining certain threshold value and it has to understand the nature of the request and need to understand the type of mode it comes under. they proposed 2 modes of behavior, they are normal by-pass mode and suspect mode. and if the router determines the packet behavior to be in normal mode then the packet will be routed to the server and if the behavior is detected as suspect mode then it will raise an alarm this mode holds the upcoming requests from the IP and later on the requests will go under CAPTCHA technique to identify between the legit user and bot and for this they proposed an algorithm for HTTP count filter where the input will be the packer headers and output will be the suspected IP's

The IPS requests that are received and lying below the threshold value will be having access to the server and the requests that are received and the requests above the threshold value will be blocked and added to the Black listed IP list and a warning is issued to the hacker in the form of response

And later in the suspect mode while undergoing CAPTCHA technique the will undergo an algorithm proposed it is they IP will receive a Captcha text to solve and a time limit will be given if the reply given by the user was correct and he replied it within the time then the request will be routed to the server otherwise the IP will be blacklisted and updated accordingly in all the IP tables to drop the request from the IP

Conclusion:

The idea proposed here is to counter back the attacks done by the hacker by spoofing his IP so that we will be blacklisting his Host IP and dropping the requests and also we need to verify the request before blacklisting using captcha technique to infiltrate humans from bots so that we will be able to give access to the legit users by blocking botnets to make the server busy.

Title: A New Security Trust Model for Peer-to-Peer E-commerce (18BCE0515)

Methodology:

P2P trust model is currently classified into the following categories:

1) The centralized trust models. The small numbers of super peer in P2P system are responsible for the supervision, periodic notice of violation peers. The system is centralized, and has some problems like poor expansion; single point failure, etc, such as eBay [1], PKI based trust model [2].

2) The role-based trust model [3]. In such systems, according to their interest, the peers join the different communities. These communities are the collection of peers with the common interest.

The same peer can join the different communities. The trust degree in different aspects is decided by the grade of membership of peers in different communities.

3) Overall trust degree model. In order to gain the overall trust degree, these models gain them through the mutual satisfaction of neighbor peers, such as the Stanford University EigenRep [4] the overall trust model.

4) The negative feedback-based trust model [5]. The malicious users in the system are a few, so the system only submits dissatisfied report c (p, q). The model only collects the part assessment on calculating trust value. More many for the dissatisfied peers, lower credibility for peers. P2P e-commerce trust model should not only consider the special nature of P2P networks model, but also consider the specific application of e-commerce environment. P2P users in e-commerce environment have the characteristic of anonymity and dispersion. When the two users decided trading, direct data transfer or other actions will be taken. In addition to the common risks of e-business, owing to its own characteristics, P2P e-commerce has also brought risks, such as the selfishness and anonymity of peers, arbitrary of identification, etc. Therefore, the trust model is proposed in this paper to quantify and evaluate P2P e-commerce in each entity, making the entity know more about the trading subject before engaging the transaction so as to enhance the security of transactions

A The definition of trust model:

Definition 1: Let DTij be the direct trust degree of peers i to peer j. It is the trust degree stemmed the past transactions behavior from the two peers.

Definition 2: For any two entities with transaction experience, it can use this method to calculate the trust value of two sides, accordingly make the judgment whether to transact with them. However, if there is no transaction or dealing with less experience between two entities, they need the recommendation of other entities, and integrate the recommendation value to calculate the indirect trust value. In this model, indirectly recommended trust vote is calculated by adopting vote agreement.

Conclusion:

This paper proposes a new trust model of ecommerce security which is based on voting agreement. It can evaluate and predicate the action of the opposite according to the two-side trading experience and recommendation of other peers. We use Matlab6.0 to simulate to detect trust model, and make contrast with EgienRep model. The results show that the trust model can more accurately evaluate the trading side of e-commerce to ensure the security of the transaction and enhance the level of security and protection in the whole network that e-commerce transaction can conduct safely. At the same time, it also solves the problem of trust degree about the no history peers, making P2P grid e-commerce more flexible, safe, stable and vigorous.

Title: An enhanced e-commerce trust model for community based centralized systems. (18BCE0515)

Methodology:

In the E2CTM model, trustors gain trust in trustees based on their previous purchase behavior in their own transactions along those of other trustors. The proposed model supports a number of critical issues. A trustor having little experience with a trustee can use the experiences of other trustors to come to a decision. Also, a trustee who is good for a certain trustor, even one with an otherwise poor reputation value, can continue transactions with that trustor. In the other words, a trustor can continue transacting business with one trustee even if other trustors do not wish to do so. Moreover, in the E2CTM model, if a trustee with a good reputation value abuses his good reputation and performs a fraudulent transaction, all other transactions with other trustors will be affected because it will be reported as soon as possible. This helps an ecommerce system prevent fraud and makes it more reliable A trustor should compute a trust value for every transaction (Trust_Val) with a trustee.

Trust_val is defined as:

$$TrustVal = (1 - \alpha)\ Reputation + \alpha LocalTrust \quad (1)$$

where α is LocalTrust+1/2 when Reputation < LocalTrust, and 2−Reputation/2 when LocalTrust ≤ Reputation. Here, local trust (LocalTrust) is the degree in which a trustor trusts a trustee. Reputation identifiifies trustee reputation according to other trustors' LocalTrust. LocalTrust is determined after a transaction is completed. First, each trustor evaluates trustee behavior for that transaction and scores it as: distrusted, partially distrusted, undecided, partially trusted, or trusted. This type of trust expression relates to a discrete trust model.

Afterward, the trustor determines a LocalTrust value for the trustee by averaging that trustee's current trust value and former trust value, is shown as:

$$LocalTrustNew(a, k) = \beta LocalTrustCurrent(a, k) + (1 - \beta)LocalTrustOld(a,k)$$

where a is a trustor and k is a trustee. Here, $0 < \beta < 1$ determines the impact of trustee current trust value and former trust value on the new LocalTrust value. This value decides how fast LocalTrust builds up or collapses. To determine Reputation, for each transaction, the trustee reputation for the most recent transaction was computed and then the new and former reputation values were averaged. The new average value will be used as the Reputation value. Reputation $Recent(k) = sigmal \in Rater(k)\ LocalTrust(l, k)/|Rater(k)|$ the overall Reputation value of a trustee, k, is computed as the average of a trustee's recent Reputation value and the former Reputation value, is shown as

$$Reputation(k) = \gamma\ ReputationRecent(k) + (1 - \gamma)ReputationOld(k)$$

where γ is the impact of a trustee's recent reputation value and former reputation value on the overall Reputation ($0 < \gamma < 1$).

Conclusion:

This study examined e-commerce business transactions that required trust to be conducted. A model was proposed (E2CTM) to embed the trust concept into e-commerce transactions. This trust model can be implemented in a wide range of applications from a small business environment such as micropayment systems to a large marketplace such as an electronic shopping system. In this paper, we applied the model to an online auction electronic shopping system.

Title: Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents (18BCE0515)

Methodology:

The proposed trusted relationships, we introduce a multi-dimensional trust construct measuring individual trust in the information system or system trust, and individual trust in the relationship with the other entities or relationship trust. Trust in the system is further differentiated into 1) security trust, 2) privacy trust, and 3) system logic trust.

Security trust is defined as the belief that the information system will be safe from hacking and the introduction of viruses or other malware. For example, a user who trusts the system security expects to use the system without introducing viruses or other unsafe software effects into their machine. User systems compromised by security malware might be used as zombies to support email spammers or denial of service attacks. Privacy trust is defined as the belief that personal information entered into a system will remain private. For example, concerning tax preparation software, a user who rusts system privacy mechanisms expects that no personal tax information will be divulged to unauthorized people or systems. User systems with compromised privacy might provide others with social security numbers, credit card numbers or other private information.

An individual using an information system to prepare a tax return for filing is vulnerable in three ways: 1) system security - the end user system may be compromised by hackers or subject to the introduction of viruses and other malware such as Trojans, 2) privacy - private and sensitive information entered into and stored in the system or transmitted by the system may be accessible to unauthorized persons, and 3) software logic - depending on the complexity of the domain, the user may rely on the accuracy of the final product provided by the system and may not have any means to verify the system output. The inclusion of security trust, privacy trust and logic, trust as elements of system trust. These are the two dimensions of relationship trust. Applying the definition of trust from above, trust in the creator of the system and trust in the associated entity are both necessary because both relationships may result in harm to the system user different types of antecedents correlate more or less strongly with the different dimensions of trust. For example, individual trust in system security or privacy may depend more on technological

antecedents than knowledge-based antecedents. Providing a typology for the various antecedents will help understand these relationships.

Conclusion:

The intersection of tax and technology acceptance is an important E-Government area because of its implications for policy, information system and tax professionals, as well as academic research. The research context of tax preparation is interesting because of (1) the use of software to complete tax returns by a large portion of the citizenry, (2) the necessity of security for transmittal of information during e-filing, (3) the privacy of the subject matter, (4) the current promotion of e-filing by the American tax collection agency (IRS), and (5) individual taxpayer ambivalence or negative attitude toward taxes and the government in general. We show that because of the complex domain environment and the privacy of the subject matter, a new model of multidimensional trust and novel antecedents to trust apply.

Title: A Trust Model for Security and Privacy in Cloud Services (18BCE0515)

Methodology:

The types of cloud are:

Private - In this model, that cloud base is only utilized Eventually Tom's perusing a particular association. Those clouds might be nearby or remote. The strategies utilized to authorize such private model might make executed by method for system management, administration supplier configuration, commission and Confirmation innovations alternately a consolidation for these.

Public - The framework is made accessible of the general population on the loose. Furthermore, might make accessed by whatever client that knows the administration area. In this model, no get confinement’s camwood be connected and no commission Furthermore, confirmation systems camwood be utilized. Community - A few associations might allot those cloud administrations. These benefits need aid underpinned via a particular group for comparable diversions for example, such that mission, security necessities Furthermore policies, or considerations around adaptability. A cloud surroundings operating as stated by this model might exist mainly or remotely and is regularly figured out how Toward a requisition that speaks to those groups keeping alternately Eventually Tom's perusing an outsider.

Hybrid - Includes the creation from claiming two alternately additional clouds. These could a chance to be private, group keeping our government funded clouds which are interfaced Toward a proprietary or standard innovation organization that gives portability from claiming information Also requisitions "around the forming clouds. Trust model can be classified as two ways of processes:

Authentication: One-time password (OTP) mechanism is a password that is valid only for a session or transaction. The use of multi-factor authentication with OTP reduces the risks associated with connecting to the system from a workstation not secured. OTP is like a system of

validation that provides an additional layer of security for data and information sensitive by requesting a password that is only valid for a single connection.

Anonymization: The pooling of resources is one of the main characteristics of Cloud Computing, where these resources are shared among several users of the service. This is the exact location of user data impossible to determine, which may lead to problems related to the location of data, their safety, accessibility, etc. For this, techniques should be used to ensure the privacy and confidentiality of data in transit and stored.

Conclusion:

Cloud Computing is a very promising way for its customers reduce operating, administrative and other costs. All in increasing the effectiveness, however, the adoption of this technology remains low, and this is safety issues, in particular the safety of data exchanged on the internet. In order to problems and to improve the adoption and the use of this technology. We studied the security aspects of the cloud, then we presented the various existing solutions, and to follow we will present in detail a solution based on a multiple cloud architecture. This solution provides secure access to the cloud by using the single-use password (OTP) and also ensures the security of data in transit using identity anonymization enabling the data to be analyzed and used efficiently and without worrying about their security.

Title: Building an e-government e-trust environment (18BCE0515)

Methodology:

Trust definition: Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action independently or his capacity ever to be able to monitor it) and in a context in which it affects his own action.

Need for trust: The most important concern in the Internet world (.i.e. e-Business and e-Government) is how to trust that we are buying from the right shop, we are paying the right person, we are dealing with the right entity, the items will arrive after we have paid for them, our privacy is preserved, our personal files and records are kept securely, our business process transactions are reated professionally, and that there is nobody monitoring our credit card details or our login credentials. These are the issues the networking environment has to resolve before we put our faith in the Internet transactions system.

Trust concerns: Trust is a central defining aspect of many economic and social interactions. “Building trust is a core requirement for establishing new relationships concerning security, confidentiality, integrity, non-repudiation, trust, etc, especially in an online virtual environment. Trust elements: The degree of trust, processes, procedures, and actions that are required to build a partnership and relationship between a government and its customers vary according to the relationship strategic significance or risk. Cultural fit and process alignment between partners are

critical trust elements in strategic partnerships and require significant staff involvement to evaluate properly.

Information technology security: In E-Commerce or E-Government, much security seems to focus on trusting the other part in the exchange. From a security perspective, trust is the result of applying a combination of IT controls.

Process automation: Using new technologies represent new possibilities and challenges at the same time for businesses.

Policies and procedures: Policies and Procedures followed by e-Government are very important to strengthen trust between exchange parties. They include internal policies and procedures concerning business process implementation, accountability, responsibility, transparency, preserving privacy, compliance investigations expose punishments and precautions taken to keep personal information safe and secure.

Legislation and legal cover: It involves the canonical form of the government performance which is the legal part of eGovernment, where new procedures and other government activities have to be formally regulated by issuing laws, bylaws, directives, and rules.

Need for legal covers: e-Governance in the department's context will focus on ensuring that existing strategies and policies are updated to address new kinds of internal and external relationships and to exploit new delivery channels.

Legal cover and trust relationship: The only way to preserve rights and build trust between both communicating parties is to legalize the process by setting the legal framework for electronic transactions and its consequences. Once the canonical for has been identified, the trust can be solely built. The foundation stone in implementing e-Government is trust, and the foundation stone in trust is the legal framework.

Trust model: the most common concerns in a reliable manner that proofs the truth of the model

Title: Building a Trust Model for Generating and Validating Assurance Keys between Consumers in E-Commerce (18BCE0515)

Methodology:

The consumer begins to enter the website; if the consumer is already registered then the consumer can log in. However, if the consumer is new (not registered before), then they start by completing the registration form that includes nationality, the national number, mobile number, date of birth and address, and their image to be uploaded from a file or webcam. Then the national number and mobile number are encrypted so that data can be sent to the TTP

TTP receives the data and decrypts the national number and mobile number, and then validates the data by reference to a Governmental body (e.g. civil affairs) and considers TTP. If data are not matching, a message will be sent to the consumer's mobile number, informing that the data is invalid and to try another one. TTP saves its data in App-Fr-DB file where the image is saved in

image-DB file by its AK number. A message will be sent to the consumer ‘s mobile phone with AK number to be used in verification of the consumer when making a sale or purchase Generating both parts without repetition and adjust all the generated random numbers to be 12-digits, as in the following algorithm:

1. Read the number of random numbers that need to be generated(amount).

2. Read the minimum value of the range (MIN).

3. Read the maximum value of the range (MAX).

4. Define the range, it must be at least equal to the amount.range=(MAX-MIN)+1;

5. Generate a uniqe random number inside the specified range, about storing the generated numbers into array to check if the number exists in the array or not before storing in the array at each generation step

6. Store the generated numbers into array

7. Function to compute the length of generated numbers.

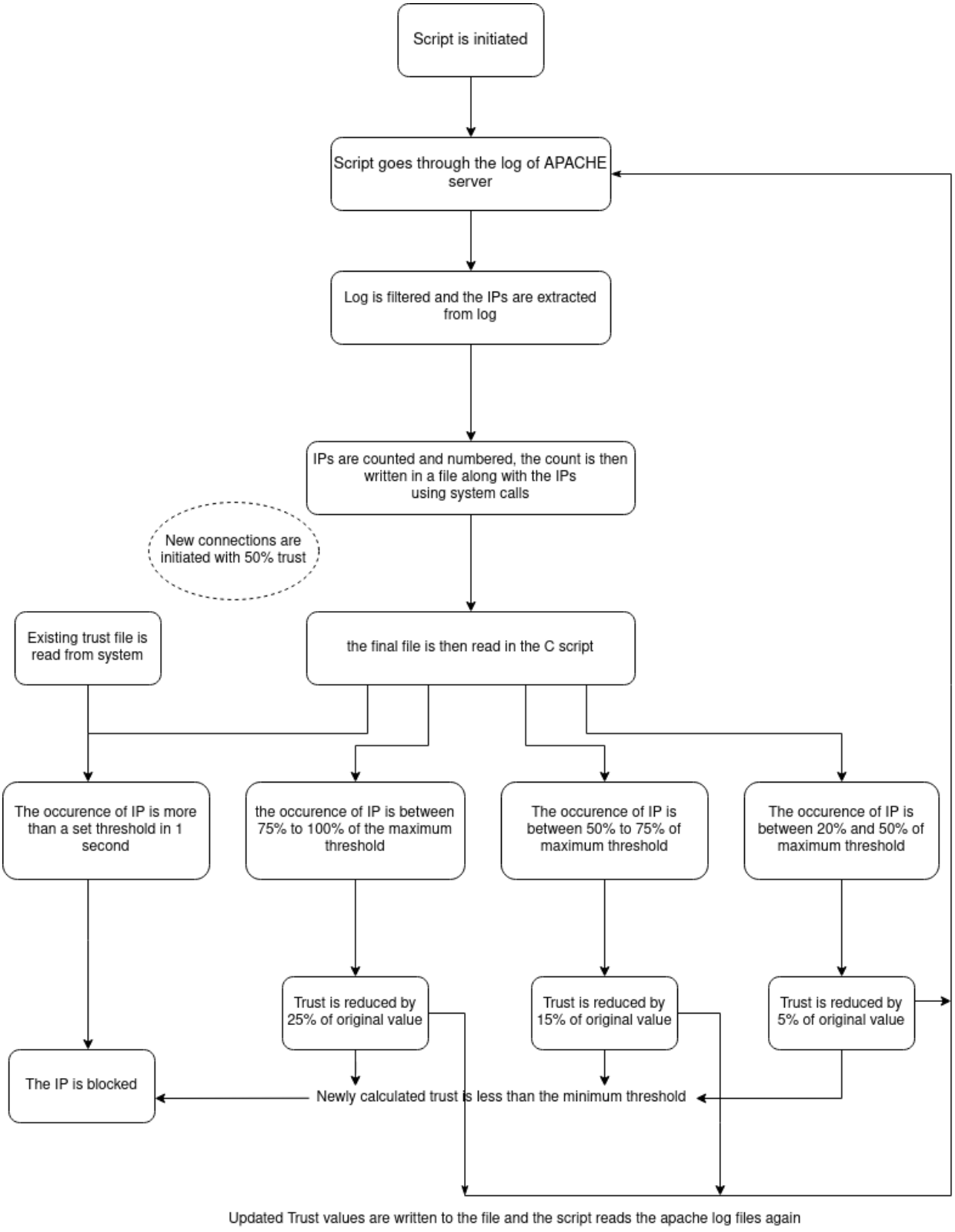
8. Complete the length of generated numbers by zeros from left to be equal in length, 12-digits.

To test this methodology, they have designed a program to read one million numbers of the random component of (20 box) to determine the proportion of the numbers that can be achieved here all the conditions form AKS, and we repeated this process 10 times, and then we extracted the average per account. Then we introduced random numbers according to the length of the numbers in each card as shown, to determine the proportion of the numbers that can be achieved where all the terms of each card in terms of the prefix and the length of the number and the equation of verification used is in the cards shown. And we repeated this process 10 times for each type of card, and then we extracted the average expense ratios for each card and compared with the results we reached in the generation of AKS. The results were as shown.

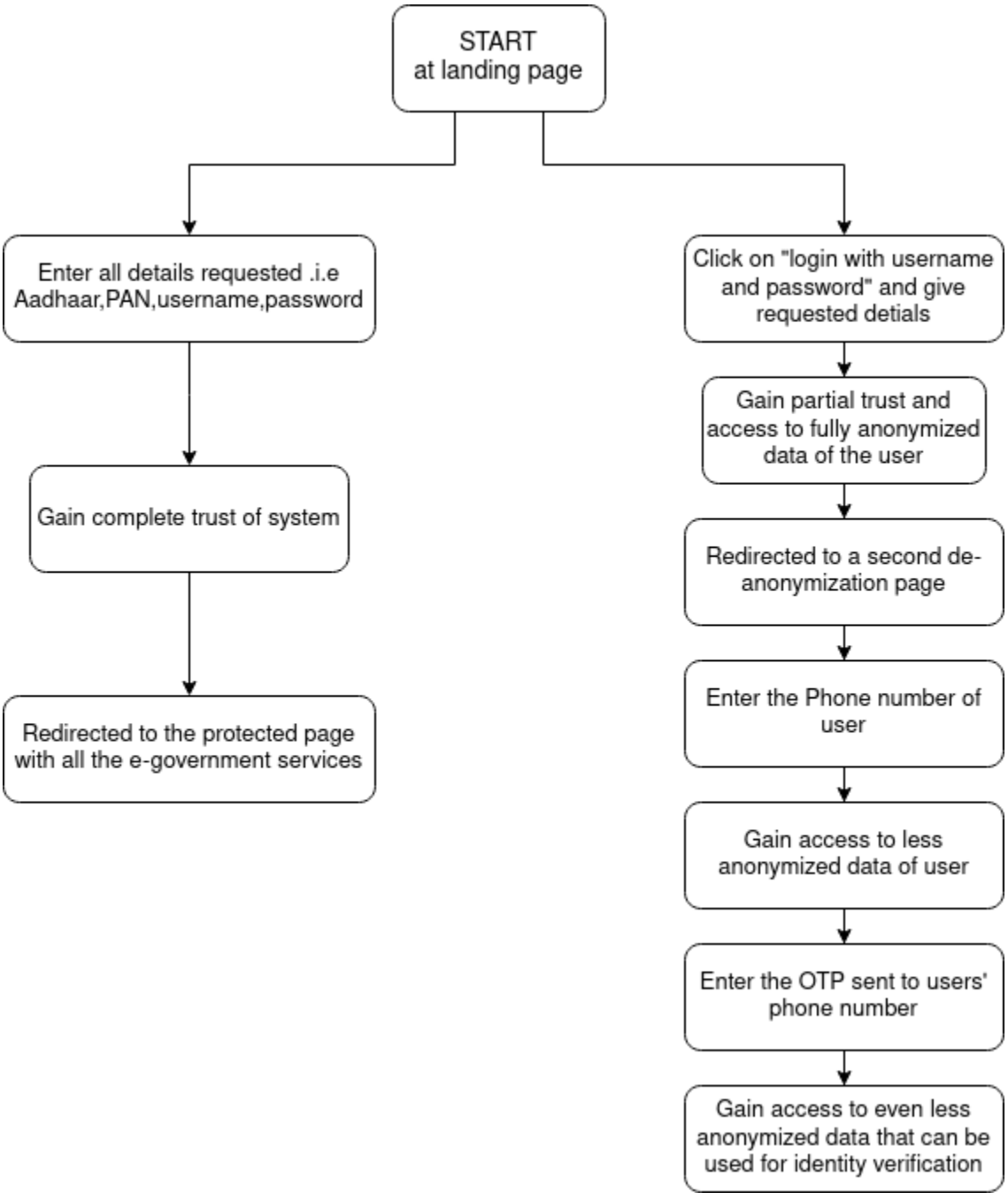
Conclusion:

This paper aims to identify the features and limitations, of a number of models employed in the field of E-Commerce pertaining to trust building between consumers. It was found that the eBay model addressed most of the limitations in previous models. However, it still has its own limitations concerning the online registration process that does not verify the user's ownership of the card. We presented a model to address this limitation by proposing a new algorithm for generating a series of unique random AK's numbers for all the consumers in the world. It saves the image of the consumer in the database of AK-DB file by its AK, and sends SMS to the consumer by AK.

Flow chart of DOS prevention script :



Flowchart of websites' trust model :



Implementation:

- The prerequisites for running the designed framework are apache httpd server, php backend, php mysql connector, gcc-c++ and mysql database connection for maintaining the user database.
- Configure the Apache server to server requests over TLS/SSL connection to increase the security of an application because we are dealing with sensitive information of a citizen. i.e to do this we have used mod_ssl. this package configures the default requests to be served over HTTPS instead of HTTP.
- now reloacte the designed website or webapp files over to the /var/www/html/ folder.
- Starting the webserver:
  - `service httpd start`
- Compiling the DOS prevention script can be done by (This has to be done only the first time, from second time we can skip this step)
  - `g++ main.c -o dosp`
- For running the code after compiling it
  - `sudo ./dosp`
- The code starts with all the include statements to import libraries. These are the required libraries for the code to run.

```
#include<string>

#include<iostream>

#include<fstream>

#include<vector>

#include<chrono>

#include<thread>

#include<algorithm>
```

- In the next block of the given C code we have written a function to block a fraudulent IP address at the Transport layer of the OSI structure. This function blocks a specific IP address by discarding any packets that were sent to the system from an unwanted IP address on any network interface.
- This function works such that the same IP can’t access any other service hosted on the same server or IP address even after the web server application has been closed because the ban is at a system level and only a system administrator can re-authorize the user to gain access to ping this IP address or request a connection from this IP address.
- Code snippet for the blocking function:

```
void block(string IP){
string bi="iptables -A INPUT -s ";
```

```
string tail=" -j DROP";
string p = bi+IP+tail;
system(p.c_str());
}
```

- Then a system command that has been invoked to run on the system using bash has been written to first take the log from system and filter it for any sequence of numbers that is an IP address.
- This line then has the code to filter out the hits from localhost that were sent by the systems in the subnet or the local admin checking on the server.
- This is then output into a file that is then opened by another set of tools that read the file, sort the IPs, then merge the IPs that have repeated and append the count at the end after a space.

- Code snippet for the above described three functions:

```
system("cat access.log | grep -oE \"\\b([0-9]{1,3}\\.){3}[0-9]{1,3}\\b\" | grep -v \"127.0.0.1\" > IPs.txt && sort IPs.txt | uniq -c | sed -e 's/^\\s*//\' -e \'/^$/d\' > uip_c.txt && awk '{for(i=1;i<=2;i++) {name=FILENAME\"_\"i;print $i> name}}' uip_c.txt");
```

- The above file is then read by the native C code and it is passed through the trust calculation process.
- Trust calculation process:
    - Older existing trust values file is opened in the native code.
    - This process can only see the IP address and the number of times that IP address has requested the server for a connection.
    - If the number of times an IP address has occurred in the system is above the maximum threshold set by the system admin in the code or if the existing trust of an IP address is below the Threshold and it hasn’t been blocked, then the function that blocks the IP address at the transport layer is invoked and the IP is banned.
    - If the number of requests is not greater than the upper threshold but the number is significantly higher than acceptable level or very close to the upper threshold the Trust value of that IP address will be reduced by 25% of original value, this way the traffic from this IP will be banned after about 10 to 20 requests from the user.
    - If the number of requests is not close to acceptable level but it is considerably higher, Then the trust will be decreased by 15% of original value.
    - If the number of requests is close to the lower threshold but somewhat higher than the lower threshold then the trust will be decreased by 5%
    - Code for this is :

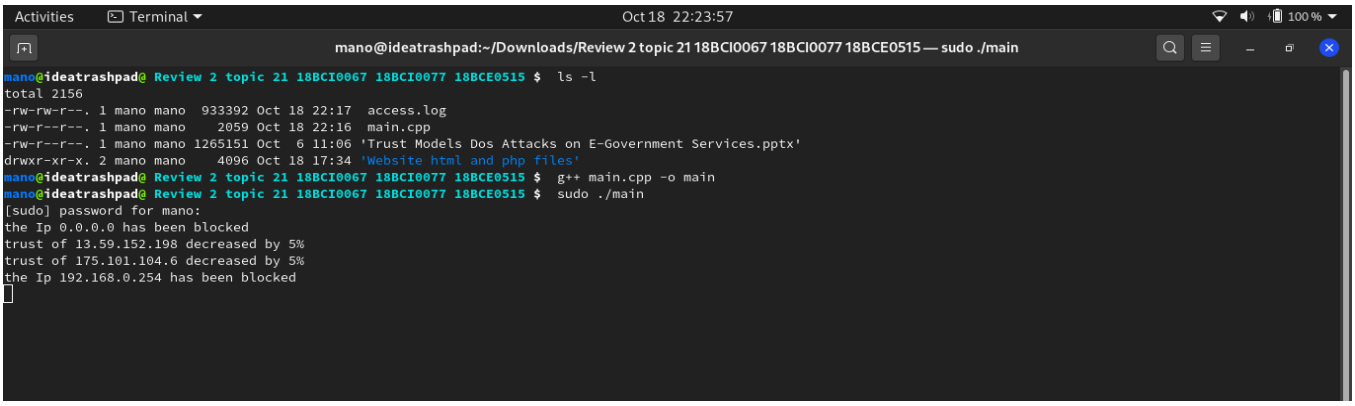
```
        if(trust[i] < 0.2 || hits[i]>=50){
        block(ipsv.at(i));
        cout << "the Ip " << ipsv.at(i) <<" has been blocked" <<
endl ;
        }
        if(hits[i]>25 && hits[i] < 50){
        trust[i]=trust[i]-(0.15*trust[i]);
        cout << "trust of "<< ipsv.at(i) << " decreased by 25%" <<
endl;
        }
        if(hits[i]> 15 && hits[i] <= 25 ){
        trust[i] = trust[i]-(0.1*trust[i]);
        cout << "trust of "<< ipsv.at(i) << " decreased by 10%" <<
endl;
        }
        if(hits[i]>=8 && hits[i]<=15){
        float tmptr = trust[i];
        trust[i] = trust[i]-(0.05*trust[i]);
        cout << "trust of "<< ipsv.at(i) << " decreased by 5%" <<
        endl;
        }
        }
```

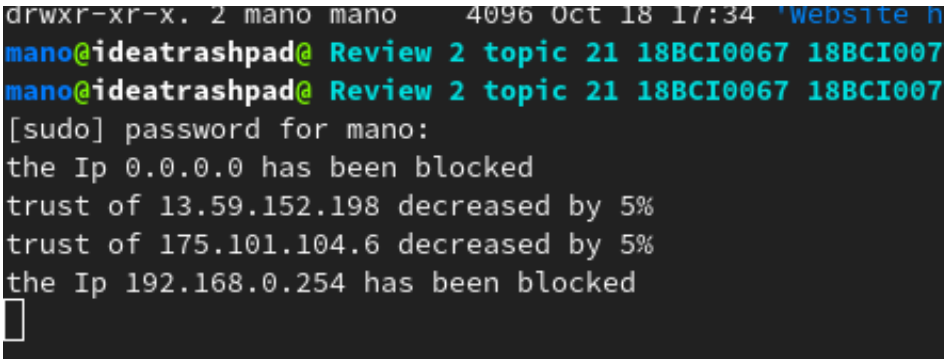
- The updated trust value will then be written back to the file and stored for future iterations.
- The code will move all the contents of the log file to another file to prevent reprocessing the same old IP addresses.
- The script will wait for a second before running again for limiting the I/O usage of the system.
- The next thing in the framework is configuring APACHE server and MySQL to limit users from accessing information that they are not supposed to access.
- Any user will have to provide some personnel information that has been stored in the database to get access to all the information.
- This way we can ensure that some random adversary that knows the password will not get access to the system.

- If the user chooses not to give governmental personal information then they can give just username, password and phone number to get anonymized data.
- If they choose not to give phone number then they will get even more anonymized data.
- The amount of anonymization can be controlled by the database manager.

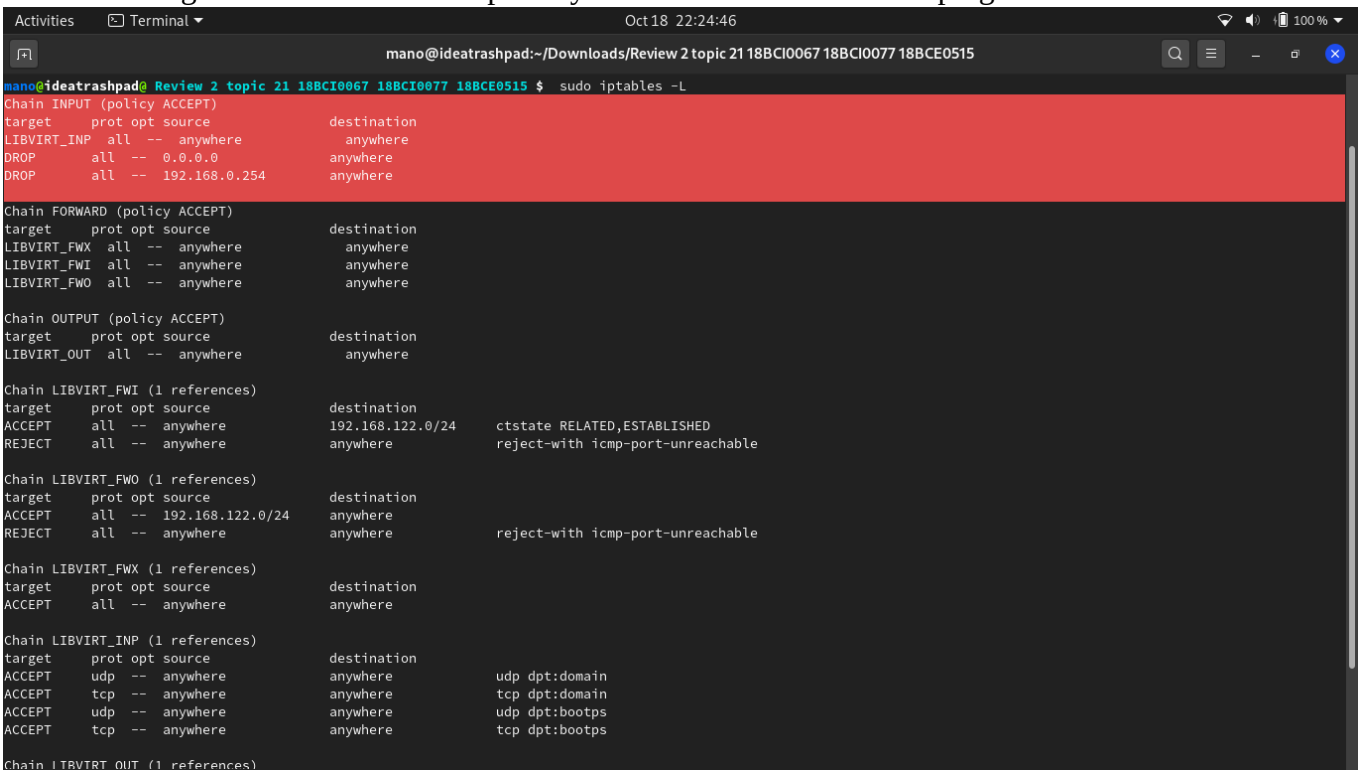
RESULT and IMAGES:

- Script reading the log and banning some IP's and decreasing the trust of some IP addresses

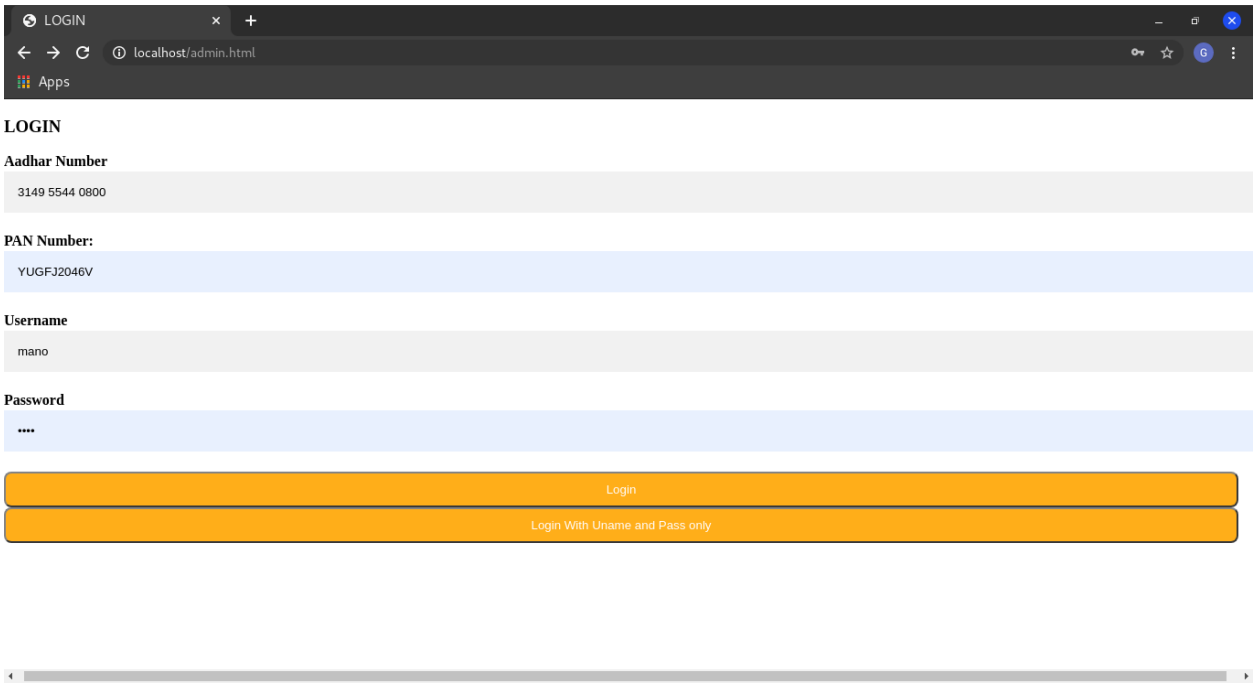




- The blocking has been done at transport layer and those IPs can’t even ping the server

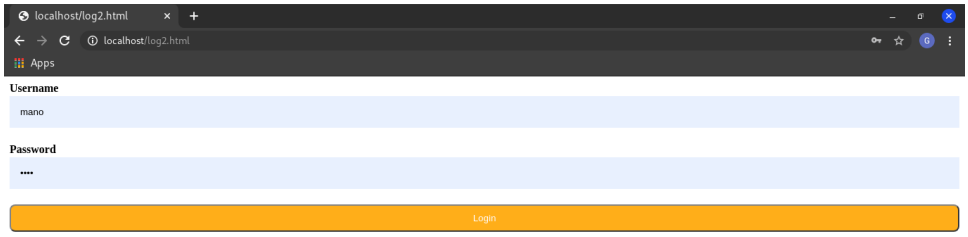


- Now visit the site that has been active on your systems IP. This can be done by typing https://127.0.0.1/ in the browser's URL box



- Now on giving the details and clicking login we get

- Or if we want to skip on the details and just proceed to see somewhat anonymised data for identification or verification purposes we can click on login with username and password on clicking that option we get



- On clicking login, we get some anonymized data and the ability to get somewhat un-anonymized data by providing phone number for verification.

- On giving phone number and clicking request we get details like

- On clicking the bypass button we get anonymised data

Aadhar Number:XXXX XXXX XXXX XX00

Age:50-100

PAN Number:XXXXXXXX6V

ZIP Code:8**

City Of Birth:Italy

Conclusion:

This project has proposed a Trust framework that has been applied on the APACHE server that can prevent a DOS attack from saturating the servers network interface and a portal has been designed based on trust framework that trusts users only when they provide some information, we have endorsed a 3-factor authentication I.e AADHAR number, PAN number and password. All of this is sent over a TLS encrypted network so that the data can't be read by any adversary.

We ran some tests on the deployed framework to ensure its effectiveness. In our testing environment the code shown perfect success rate.

Work division:

DOS_PREVENTION code: 18BCI0077

Trust model for the WEBAPP : 18BCI0067

Server configuration : 18BCE0515

1. Abstract – 18BCI0077 Gogireddy Manohar
2. Introduction – 18BCI0077 Gogireddy Manohar
3. Motivation – 18BCI0077 Gogireddy Manohar
4. Literature review --
    - 4.1. 18BCI0077 Gogireddy Manohar
        - 4.1.1. Security Engineering for E-Government Web Services: A Trust Model
        - 4.1.2. E-Government and Cloud: Security Implementation for Services
        - 4.1.3. A trust model based on theory of evidence for E-commerce environment
        - 4.1.4. A Collaborative Trust Model of Firewall-through based on Cloud Computing
        - 4.1.5. Study on Double-Layers Trust System and Model of Trust in P2PEB mode

4.2. 18BCI0067 Dodda Sumanth

4.2.1. DDOS Attack Detection and Mitigation Technique Based on Http Count and Verification Using CAPTCHA

4.2.2. A P2P-based Trust Model for E-Commerce

4.2.3. A Cloudlet based security and trust model for e-government web services

4.2.4. TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs

4.2.5. Beyond “web of trust”: Enabling P2P E-commerce

4.2.6. A Fuzzy Trust Model for E-Commerce

4.2.7. An Integrated Trust Model for Business-to-Consumer (B2C) E-Commerce

4.2.8. Trust based secure routing mechanisms wireless sensor networks: A survey

4.3. 18BCE0515 V Venkata Narendra

4.3.1. Building a Trust Model for Generating and Validating Assurance Keys between Consumers in E-Commerce

4.3.2. Building an e-government e-trust environment

4.3.3. A Trust Model for Security and Privacy in Cloud Services

4.3.4. Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents

4.3.5. An enhanced e-commerce trust model for community based centralized systems.

4.3.6. A New Security Trust Model for Peer-to-Peer E-commerce

References:

[1] Al-Shargabi BA, Al-Jawarneh SH, Hayajneh SM. A cloudlet based security and trust model for e- government web services. Journal of Theoretical and Applied Information Technology. 2020 Jan

15;98(1):27-37.

[2] B. Alessandro, R. Barbara and P. Alberto, "E-government and cloud: Security implementation for services," 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG), Quito, 2017, pp. 79-85, doi: 10.1109/ICEDEG.2017.7962516.

[3] G. Himanshu and K. Desire Afewou, "A trust model for security and privacy in cloud services," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, 2017, pp. 443-450, doi: 10.1109/ICRITO.2017.8342468.

[3] Kerrache, Chaker Abdelaziz, et al. "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs." Vehicular Communications 9 (2017): 254-267.

[4] B. Al-Shargabi, "Security Engineering for E-Government Web Services: A Trust Model," 2016 International Conference on Information Systems Engineering (ICISE), Los Angeles, CA, 2016, pp. 8-11, doi: 10.1109/ICISE.2016.17.

[5] K. J. Singh and T. De, "DDOS Attack Detection and Mitigation Technique Based on Http Count and Verification Using CAPTCHA," 2015 International Conference on Computational Intelligence and Networks, Bhubaneshwar, 2015, pp. 196-197, doi: 10.1109/CINE.2015.47.

[6] Abbass SM, Ibrahim OB, Farag MS. Building a Trust Model for Generating and Validating Assurance Keys between Consumers in E-Commerce. International Journal of Computer Applications. 2012 Jan 1;57(1).

[7] Abbass SM, Ibrahim OB, Farag MS. Building a Trust Model for Generating and Validating Assurance Keys between Consumers in E-Commerce. International Journal of Computer Applications. 2012 Jan 1;57(1)

[8] Morid, M.A., Shajari, M. An enhanced e-commerce trust model for community based centralized systems. Electron Commer Res 12, 409–427 (2012).

[9] W. Xu and G. Yucui, "A trust model based on theory of evidence for e-commerce environment," 2011 International Conference on E-Business and E-Government (ICEE), Shanghai, China, 2011, pp. 1-3, doi: 10.1109/ICEBEG.2011.5881920.

[10] Z. Shaolin and Z. Fan, "Study on Double-Layers Trust System and Model of Trust in P2PEB Mode," 2011 Fifth International Conference on Management of e-Commerce and e-Government, Hubei, 2011, pp. 39-42, doi: 10.1109/ICMeCG.2011.59.

[11] Z. Yang, L. Qiao, C. Liu, C. Yang and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," The 2010 14th International Conference on Computer Supported Cooperative Work in Design, Shanghai, China, 2010, pp. 329-334, doi:10.1109/CSCWD.2010.5471954.

[12] Mcleod, Alexander & Pippin, Sonja. (2009). Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents. Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS. 1 - 10. 10.1109/HICSS.2009.380.

[13] Al-Dwairi, Radwan M., and Mumtaz A. Kamala. "An integrated trust model for business-to-consumer (b2c) e-commerce: integrating trust with the technology acceptance model." 2009 International Conference on CyberWorlds. IEEE, 2009.

[14] Yu Wang, Wang Yu, Zhao Yue-long and Hou Fang, "A New Security Trust Model for Peer-to-Peer E-Commerce," 2008 International Conference on Management of e-Commerce and e-Government, Jiangxi, 2008, pp. 399-402, doi: 10.1109/ICMECG.2008.86.

[15] Al-Hussein, Hussein & Omari, Ahmed. (2006). Building an e-Government e-Trust Infrastructure. American Journal of Applied Sciences. 3. 10.3844/ajassp.2006.2122.2130.

[16] C. Su, H. Zhang and F. Bi, "P2P-based Trust Model for E-Commerce," 2006 IEEE International Conference on e-Business Engineering (ICEBE'06), Shanghai, 2006, pp. 118-122, doi: 10.1109/ICEBE.2006.78.

[17] Nefti, Samia, Farid Meziane, and Khairudin Kasiran. "A fuzzy trust model for e-commerce." Seventh IEEE International Conference on E-Commerce Technology (CEC'05). IEEE, 2005.

[18] Datta, Anwitaman, Manfred Hauswirth, and Karl Aberer. "Beyond" web of trust": Enabling P2P E-commerce." EEE International Conference on E-Commerce, 2003. CEC 2003.. IEEE, 2003.

[19] EA, Mary Anita. "Trust based secure routing mechanisms for wireless sensor networks: A survey." 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2020.

CODES:

DOS-prevention :

Main.cpp :

```
#include<string>
#include<iostream>
#include<fstream>
#include<vector>
#include<chrono>
#include<thread>
#include<algorithm>
using namespace std;
void block(string IP){
    string bi="iptables -A INPUT -s ";
    string tail=" -j DROP";
    string p = bi+IP+tail;
    system(p.c_str());
```

```
}
int main(){
    std::vector<float> trust(100,0.5);
      system("cat access.log | grep -oE \"\\b([0-9]{1,3}\\.){3}[0-9]
{1,3}\\b\" | grep -v \"127.0.0.1\" > IPs.txt && sort IPs.txt | uniq -c
|   sed   -e   's/^\\s*//\'   -e   \'/^$/d\'   >   uip_c.txt   &&   awk
'{for(i=1;i<=2;i++){name=FILENAME\"_\"i;print $i> name}}' uip_c.txt");


    //read number of hits from each ip into a vector
    ifstream hfile;
    hfile.open("uip_c.txt_1");
    std::vector<int>hits;
    int number;
    while(hfile >> number)
    hits.push_back(number);
    hfile.close();


    //read IP from files into a vector
    vector<std::string> ipsv;
    ifstream ipfile;
    ipfile.open("uip_c.txt_2");
    string str;
    while (std::getline(ipfile, str))
    {
        if(str.size() > 0)
            ipsv.push_back(str);
    }
    ipfile.close();


    system("rm IPs.txt 2> /dev/null && rm uip* 2> /dev/null");
    for(int i=0;i<ipsv.size();i++){
```

```
        string txtf = ipsv.at(i);
                int  pos  =  distance(ipsv.begin(),  find(ipsv.begin(),
ipsv.end(),txtf));
        trust[i]=trust[pos];
    if(trust[i] < 0.2 || hits[i]>=50){
            block(ipsv.at(i));
             cout << "the Ip " << ipsv.at(i) <<" has been blocked" <<
endl ;
        }
        if(hits[i]>25 && hits[i] < 50){
            trust[i]=trust[i]-(0.15*trust[i]);
            cout << "trust of "<< ipsv.at(i) << " decreased by 25%" <<
endl;
        }
        if(hits[i]> 15 && hits[i] <= 25 ){
            trust[i] = trust[i]-(0.1*trust[i]);
            cout << "trust of "<< ipsv.at(i) << " decreased by 10%" <<
endl;
        }
        if(hits[i]>=8 && hits[i]<=15){
            float tmptr = trust[i];
            trust[i] = trust[i]-(0.05*trust[i]);
             cout << "trust of "<< ipsv.at(i) << " decreased by 5%" <<
endl;
        }
    }
    system("cat access.log >> access.log.bak && >access.log");
    std::this_thread::sleep_for(200s);
return 0;
}
```

PHP backend for the Webserver:

PHP –1:

```
<?php
$servername = "localhost";
$usern= "18BCI0077";
$passw= "Man0h@r0";

// Create connection
$conn = new mysqli($servername, $usern, $passw,'secproj');

// Check connection
if ($conn->connect_error) {
  die("Connection failed: " . $conn->connect_error);
}
else{
    $u=$_POST['username'];
    $p=$_POST['password'];
    $adh=$_POST['aadhar'];
    $ph=$_POST['pannumber'];
       $adhsql=$conn->query("select  Aadhar_Number  from  secproj  where username='$u' and password='$p'");
    $adhh=$adhsql->fetch_row();
    $adhhh=$adhh[0];
    echo $adhhh;
          $phnn=$conn->query("select  PAN_Number  from  secproj  where username='$u' and password='$p'");
    $phnnn=$phnn->fetch_row();
```

```
    $Phn=$phnnn[0];
    echo $Phn;
          $sql="select   *   from   secproj   where   username='$u'   and
password='$p'";
    $result=$conn->query($sql);
        if($adh==$adhhh && $Phn == $ph ){
            if($result->num_rows>0){
            header("Location:sucess.html ");
            }}
        else
            {header("Location: admin1.html");}

    }
?>
```

PHP –2:

```
<?php
session_start();
$servername = "localhost";
$usern= "18BCI0077";
$passw= "Man0h@r0";

// Create connection
$conn = new mysqli($servername, $usern, $passw,'mano');

// Check connection
if ($conn->connect_error) {
```

```
  die("Connection failed: " . $conn->connect_error);
}
else{
    $u=$_POST['username'];
    $p=$_POST['password'];
    $dig = openssl_digest($p, "sha224", false);
    $_SESSION['id']=$u;
    echo $p;
    $sql="select * from secb where username='$u' and pa_hash='$dig'";
        $result=$conn->query($sql);
        if($result->num_rows>0){
            header("Location:mob.html ");
            }
        else
            {header("Location: log21.html");}

}
?>
```

ANON-1.php:

```
<?php
    session_start();

    $connect=new mysqli('localhost','18BCI0077','Man0h@r0','mano');
    if($connect->connect_error){
        echo "connection failed";
    }else
    {
```

```
        $q=$_SESSION['id'];
               $sql1="select  *  from  anon3  where  username=('$q')"or
die(mysql_error());
        $res=$connect->query($sql1);
        while($row=$res->fetch_assoc())
         {
          echo "<h1>"."Aadhar Number:".$row['Aadhar_Number']."</h1>";
          echo "<h1>"."Age:".$row['age']."</h1>";

          echo "<h1>"."PAN Number:".$row['PAN_number']."</h1>";
           echo "<h1>"."ZIP Code:".$row['zip_code']."</h1>";
            echo "<h1>"."City Of Birth:".$row['city_birth']."</h1>";




         }


    }
?>
```

ANON-2.php :

```
<?php
    session_start();

    $connect=new mysqli('localhost','18BCI0077','Man0h@r0','mano');
    if($connect->connect_error){
        echo "connection failed";
    }else
```

```
    {

        $q=$_SESSION['id'];
               $sql1="select  *  from  anon2  where  username=('$q')"or
die(mysql_error());
        $res=$connect->query($sql1);
        while($row=$res->fetch_assoc())
         {
          echo "<h1>"."Aadhar Number:".$row['Aadhar_Number']."</h1>";
          echo "<h1>"."Age:".$row['age']."</h1>";

          echo "<h1>"."PAN Number:".$row['PAN_number']."</h1>";
           echo "<h1>"."ZIP Code:".$row['zip_code']."</h1>";
            echo "<h1>"."City Of Birth:".$row['city_birth']."</h1>";




         }


    }
?>
```

ANON-3.php:

```
<?php
    session_start();

    $connect=new mysqli('localhost','18BCI0077','Man0h@r0','mano');
    if($connect->connect_error){
```

```
        echo "connection failed";
    }else
    {

        $q=$_SESSION['id'];
               $sql1="select  *  from  anon3  where  username=('$q')"or
die(mysql_error());
        $res=$connect->query($sql1);
        while($row=$res->fetch_assoc())
         {
          echo "<h1>"."Aadhar Number:".$row['Aadhar_Number']."</h1>";
          echo "<h1>"."Age:".$row['age']."</h1>";

          echo "<h1>"."PAN Number:".$row['PAN_number']."</h1>";
           echo "<h1>"."ZIP Code:".$row['zip_code']."</h1>";
            echo "<h1>"."City Of Birth:".$row['city_birth']."</h1>";




         }


    }
?>

//THIS CONCLUDES THE DRIVER CODE FOR OUR PROJECT
```