CHAPTER 1

INTRODUCTION

1.1 WEB APPLICATION

Web application has been known for years that and inexpensive channels to communicate and exchange information in the web. It has played a unique role in the life of business man, who has extraordinary prospects and multiple transactions with customers. The web, undoubtedly paves way for the marketers to get to know numerous people with plenty of communication links. As a business network, the particular web visitors are tracked to subscribe newsletter to submit applications requesting products, to give feedback to provide details about their experience with the browser. Website widgets such as submit fields, enquiry and login forms, shopping cards and content management system frame, web application, which are fundamental to businesses to create long lasting relationship with customers. Being a ubiquitous phenomenon, with technical and complex nature, web applications are normally misunderstood in cyber-life.

The web, being programmable, brings out large and diverse range of applications to millions of the globe. A modern website comprises extensive web applications and flexible web browsers. These web browsers are no doubt software applications to retrieve data and interact with the content on web pages. The reasoned web applications meet the need of the modern consumers by providing capture, processing, storage and transmission
of the clear data. Features such as web mails, login pages, request forms etc shape modern websites to communicate with the customers.

Thus web applications allow the visitor to submit or retrieve data to or from database using the internet. Web documents are dynamically generated in a specific format. Moreover they execute their functions irrespective of the operating system and the browsers running. It needs no installation requirements and is being deployed quickly.

**How do web Application work?**

The Figure 1.1 shows the N-tier web application model. The first tier is normally a web browser or the user interface; the second tier is the dynamic content generation technology tool such as Java server Pages (JSP) or Active Server Pages (ASP), and the third tier is the database containing content and customer data.
1.2 PRIMARY ELEMENTS OF WEB APPLICATION

1.2.1 Web Server

The Web server that hosts the web pages, documents or folder that need to access. This facilitate for the surfing in internet the browser will establish a connection to a reverse proxy with the help of HTTP, HTTPS. In response to that the proxy will connect to the web server through HTTP.

The server is probably going to be on the IP address, unlike in the public network here the private network allow the web server to share a database that not necessarily be exposed to the internet on public IP address.

In case of HTTPS requirement it is configured on the proxy and not on the web server. The request came from the HTTP reverse proxy will also clean in some way. For instances the length prescribed by the browser or the URL as far as the user string is concerned must not exceed the prescribed length.

1.2.2 Firewall

Firewall is pre-emptive on the part of firewall to ensure that no untoward incidents have been plotted out by the perpetrators and indulging to have both physical and logical damage to the system. And the firewall mechanism that we deploy must have the capacity to address the issues pertaining to the logical destruction of the system; it has to break- the- logjam by having denied the holistic approach towards by some hostile elements. Moreover neither the host server nor the guest server must have been given equal priority when it comes to spearheading the data flow from source to destination. Nonetheless the people have guaranteed with the state-of-the-art
technology for the network assignment they entrusted they lack the holistic approach.

**What does Firewall do?**

The firewall has to curb the network atmosphere on the bilateral basis, then only both ends either the source or destination will be covered under the protection regime. Whenever any unauthorized users attempted to intrude into the private network applications, the firewall would raise the alarm to the concerned authority by bringing the potential threats to the limelight. It can also filter the address of the origination of the data and destination of data it can be referred as address filtering, unlike the address filtering where the source and destination addresses will be taken into consideration whereas in the protocol filtering is limited only to the rules applied to realize the network. The example for those things is HTTP, FTP, and TELNET.

**What can’t the Firewall do?**

The firewall’s mandate is confined to certain areas where it can have the control over and rule from top to bottom. There are some exceptions where it can’t have the control over them, like the individual users with modulator and demodulator trying to dial through the network in an unjustifiable manner. Sometimes the people who are working for the same concern intentionally or unintentionally may fall in some mischievous acts that could not be prevented. The law enforcement agencies of the particular country sometime may require to have access to the private network application server given the firewall could not single handedly handle to thwart any potential cyber attack from the terrorists, in that context the entire functions of the firewall may go in vain. The confinement of phone master cracker has brought these issues to the limelight that they had sneaked into the
information system and run by AT&T Corp., a British telecommunication inc. The pranksters could use automated robot for random internet protocol scanning and attack the devices irrespective of personal computer or server of the company, whenever the opportunity knocks their way.

Who Needs a Firewall?

Anyone who is responsible for a private network that is connected to a public network needs firewall protection. Furthermore, anyone who connects so much as a single computer to the Internet via modem should have personal firewall software. Many dial-up Internet users believe that anonymity will protect them. They feel that no malicious intruder would be motivated to break into their computer.

How does a Firewall Work?

The access resisting mechanism we are getting out of the firewall works in two ways. The firewall would not place any hurdle across the path and on the pace of the network, unless it is met with some uncertainty like the attack of the malicious element that warrants the intervention of the firewall vice versa, the very same philosophy can be applied to not to allow any communication between the particular source and destination. The criteria followed for determining to kept the gate wide open to facilitate to manoeuvrings of data in the internet or network application system differ from one firewall to another. Its area of control may be limited to the type of traffic, source to destination address and the internet port.
Types of Firewall

Firewall has been categorized into number of firewalls namely; packet filters, circuit level gateways, application level gateways and statefull multilevel inspection firewalls. Among the various levels of OSI reference model the packet filtering deals only with the network level the considered to be the part and parcel of router. The main function of routing device is to receive packet from one network and routing through another one. The data about to be forwarded has to go through the number of criterion before it has reached the intended receiver. It is up to the firewall to decide whether to forward or not by applying the rules in place to that extent the entire power is vested upon only with the firewall. When it comes to the affordability of the packet filtering as well as the impact it wields on network performance packet filtering is the sole choice of all the stakeholders like routers. Notwithstanding has not supported the sophisticated protocols based on the rules models (Network address translation), at the lower lever like network level it could play constructive role for high degree of security.

Unlike the packet filtering, circuit level gateway works on the session layer model of the OSI reference model. Circuit level gateways would always keep its avian view that would pave the way for the session layer to ensure that the request came from the authenticated session, In other words it checks the legitimacy of the session layer. Contents reached the remote communication devices via circuit level gateway seems to have originated from the gateway. Moreover this will help to mislead the mischievous players who entered into the network pretending that they are genuine one. Last but not least the affordability, small upcoming firms can also avail this, even though they may be in deep economical mess.

If set aside application aspects of the application level gateway it would be very hard to find even a single change between the circuit level
gateway and the application level gateway. It can otherwise be called as a proxy to the circuit level gateway. It can filter packet at the application layer of the OSI reference model. Inbound and outbound packets cannot ask for services for which there is no proxy. Application level gateway that is entrusted to act as proxy will not permit the FTP, Gopher, and Telnet. They segregate the commands specific to the application layer like HTTP. Application level gateways triumphs in streamlining the entire user accessibility that will provide a full-fledged network security.

Statefull multilayer inspection firewall is a combination of the above three types of firewall mechanisms. This will filter packet at the network layer, the credibility of the session packets are confirmed and are evaluated the content by interception at the application layer level and rejuvenate the communication process by setting aside the lack of transparency in the application layer gateway.

The multilayer inspection firewall was instrumental in mooting the idea of giving end-to-end solution to any issue related to communication in network to realize the objective hassle free.

The firewall is an inseparable part and parcel of network security paradigm. Of course it has some loopholes in it. It will address the issues only to the extent of data integrity, credibility, confidentiality and authenticity of the data associated with the firewall.

1.2.3 Network Security

Network is a complex area, basically a well experienced and expertise exports only can perform such problems. However wired and wireless, increasing huge number of users needs to understand the security of
network environment. This work is expressed for basic computer users and the system organizers in mind. By explaining the process needed to read through the market place and understand deal of risk, which is not intended to a recently as well as sufficiently raised questions to accomplish a specific function.

The fundamental understanding of network is to understand the procedure of security will cover some functions of networking and then more onto some familiar networks.

Some popular networks are described in the network protocols which are public and private networks. On public anyone can link of these networks, or they can use the varieties of networks to be connected to their own hosts, without interlinking the public networks.

**Batch Processing**

Batch processing is also a similar type of batch oriented systems. Everything can be added to a unique role of queue and it specify the time, the queue basically processed based on their procedures.

**Implementation**

A Network is a group of two or more computer system linked together.
Figure 1.2 Simple network

But it builds a matter configured to the related host which is recognized by the authority. Adding a new node to the network is basically simple and would like to join networks, must be reconfigured naturally. The Figure 1.2 shows simple networks whereas the users are identified in the ways of hosts and to separate hosts and the users. The public network is simply a worldwide number of network hosts connected to each.

Familiarity

The public group of network shrinking the weight or height over the periodic interval, in the raise of expensive of availability connections additionally we are controlling connection based on yearly, monthly, weekly, daily and hours. If there is a delay occurred in the existing network, the user has to be reconfigured in a flexible manner. E.g. the files can be copied from networks, documents, emails etc. That makes the network be utilized by worldwide cases. However the people need such Netnews, emails are quite different and difficult of integration into the net has effectively decreased the no. of inconveniences that have to be accommodated.

On the other hand, security is the most important challenging feature in the world of every attributes. As far as this problem is concerned the strong points of security is inbuilt in a very limited area. Therefore more difficulties to track sometimes easily and most of the bugs are discovered, fixed and analysed. Such networks are made up of direct contact to the respective registered host only.

Typically works are under system wide users identification details (user id & password). For that, any system wants to connect a network that appropriate user has to check their used id and password periodically.
Identification of traceable points is very little that of emergency. All the hosts must have sequences number for identification.

**Inter-Networking**

Inter-networking is the world’s strongest and largest group of networks. When the users want to access the resources which are sponsored by the internet work, connection between the networks is eventually connected to the backbone of the internet, which is extremely or incredibly overflowed by the bulk of network users. Basically network is not a network of hosts but network is a network of networks.

![Figure 1.3 Local area networks](image)

The Figure 1.3 shows the construction of some protocols that are internet users’ use to interlinking to anything. Such a network might allow putting some single digit hosts or some bulk of users host on the network. Here the number of singles digit as well as group of nodes is altogether on a backbone of network of a network. That is network of networks. To use a service from any individual host we need web server and web browser connection to the host. Underlying such services and protocols can send datagram’s with the queries to the ISP network. Then a network connects to, and so on, until it finds a way to the network backbone, and exact network hosts on. The host would respond exactly the same in reverse order (The datagram’s would traverse all kind of connections until find back to the computer).
Figure 1.4 Network connections

The Figure 1.4 is designed by number of LAN, this shows how the connections on that network are needed to the connectivity to another hosts on the same LAN, within a same group, other group, but in the same ISP, cloud also from another ISP anywhere in the ISP environment internet.

Terminology related to security

IP

Internet Protocol allows the host users to allow actual talk to other user. Such datagram mapping address “9.2.4.6.” to the physical network address (01:03:11:a0: de: 4f) and routing.
The understanding of IP is a very relevant feature of network security which provides flexible protocol to focusing on the security of IP and the lake of thereof.

**Some possible attack of IP against network security**

Typically this mechanism exploits the fact of performance that does not reflect a robust mechanism for authentication, which is, evidently showing the datagram came from which location and it can claims it. These data grams simply originate from the given address, and it does not a way to be sure that host can send the datagram is telling the truth.

**Spoofing**

Spoofing means claim the IP address of another IP address. Since the system which defines the datagrams may not inform senders IP address, which is a unique useful technique for the attacker. In addition to that, the IP address of the person making request to the trustable or untreatable layer can provide security.

**Hijacking of IP Section**

Hijacking is relatively sophisticated and dangerous, however the underground community of other allowed users or unskilled bad-guy to perform this attack. IP hijacking is an attack where in the user session is over, the user was in the mid of the process of e-mail, the attacker is looking at executing commands wishes as the attacked user. For this description, the attack is with large number of networks, a user can carry a session of host and it perhaps the session of telnet. Somewhere, the network between host A and B which is run by a third party person on host which is watched by the traffic
controller, at the same time any user to shut up, convince to try longer on the network which specifically avoids the crash, mesh, network outage.

**TCP**

TCP is a protocol which needs transport layer to perform transport activities for TCP connection. To justify, IP was designed to carry among other TCP datagrams, because TCP and IP were designed together to locate wherever you are. The entire method of internet protocol is known inter collectively by TCP/IP.

**Packet delivery under guarantee**

Probability of which is a most significantly guaranteed delivery of packets. East host can send packets to their destination host and to get acknowledgement for each packets delivery. If some nodes not send an acknowledgement to the specific centre of time and it will respond the datagram packet. If some packets are missing it will reapply by the sender host and if packets reached under out of time, the recipients will arrange in clear order before sending the packet to be requested. This kind of suited application happens in telnet session, If some user wants to send sure key stoke is received from the senders remote location, and it will send back to every packets, if it means lightly change of occasional responses for same lost of packets or out of order packets.

**UDP**

UDP is a simple transport layer. It does not reflect the same features of TCP and sometimes considered as unreliability. In this kind of unsuitable applications it does not have more applicability in other applications than the robust TCP.
One of the similar things makes UDP under simplicity because it will not reflect the track of sequence of packets. It has less overhead than TCP; it means which is more suitable for data streaming applications, and also less screwing around the needs of making sure of all packets.

**Risk Management Security**

There are many extremes under absolute security and accurately access. In this closet format it can get into an absolute secure machine is one unplugged from the network, logged in safe, power supply and so on. A machine which is absolutely access under some extreme convenient to use like without asking questions, passwords, authorization and other mechanisms.

**Denial of Service**

Denial of services are more difficult to address because they are easy to launch and impossible to track, and it is not easy to refuse the users request of attackers, without refusing the request from the service. Some attacks are commonly fair become less popular it includes.

- Not visible to the globe servers at a level to close up to the capacity of the server.
- Normally packet filtering to prevent forged packet from the network address page.
- Of course forged packets would include their claims to come from their own hosts and addresses reserved for private networks.
- Making security related batches for their host operating systems up to data.
Executing commands illegally breaking the confidentiality destroying behavioural model did lying of data hijacking destructing the data.

Network Failure

Some of the processes to prevent the network failures are

- The advisors can watch the vendors saying, close watch on groups like relevant features and relative addressing details etc.
- The system can avoid single point of failures. It means the system can break any one Component which is not very strong. In security point of view it needs a degree of redundancy it can help prevent the organization from minor issues.
- The OS batches may use only current relative features.
- At least some group of people who are charged with the keep of security developments is a good idea.

Computer security is preventing and detecting the not accessed use of computer. The measure of prevention help is to quit unauthorized users who are also knows as intruders. Basic detection needs to determines whether the attempted system to break into the system, and they may have done successfully for accessing the computer system.

Using computer everything from communicating investing, shopping, email or chat program are all under considering communication of almost level of secret, in probably some strangers tracing to your email using computer information stared in the computer system.
Eventually the cracks are always displaying holes (vulnerabilities). This complexion of software which makes increasing the difficulties in parallel thoroughly checking the security of computer system.

It includes some additional links of information

- The awareness of broadband
- Modem access using physical cable connection.
- Internet connectivity using digital subscriber’s line.
- Traditional dial up services different from broadband services.

**Dial-Up**

The Dial-up network technology includes the following features

- A demand connection type.
- Dynamic changes of IP address.
- Low connection speed.
- The remote control potential under dialed into the control remotely.
- ISP-provided security under little.

**Broad Band**

The broad band network technology includes the following features

- On type connection setup.
- Static IP address changing.
- High relative connection speed.
- Any time computer can connect to the remote access under remote control potentials.

- ISP provided security under none.

Static and Dynamic Modes

The static IP address presents under presents under ISP permanent assigning more than one IP addresses for every user. If a static address is assigned but not in use under the case of do not change the time. Since it has limited number of allotment from the specific address locations and it sometimes make it efficient use of address. Dynamic utilizes their ISP space using dynamic IP of individual user computer may change over the time.

Network Address Translation

Network address translation provides a way to hide IP address of the internet while allowing computer on the network to access the internet. A NAT can be used in many ways but some method do not adopt frequently used by the home users. In the same way the telephone number of physical number may be associated with more than number of person, a user may have multiple number of applications running on their IP address under same.

Antivirus

Variety of antivirus packages that operates in different ways depends on their choice to implement software. Computer can indicate the presence of known intruders.

- Confidentiality- information should be available in right kind of access.
- Integrity-authorized user’s information only present.
- Availability—when the needed information should be accessible in the accessed users.

**Misuse of Computer Network**

The ways of misusing the network are

- Sniffing of packets.
- Spoofing of email.
- Mesh of scripting.
- Unprotected sharing of windows. e.g. java, JavaScript and antivirus.
- Virus of email.
- Extension of hidden files.
- Unauthorized users of mobile quotes.

**Accidents of Risks**

The following are the causes of network failure

- Failure of disk.
- Failure of power.
- Theft of physical components.
**Action of Protecting Computer System**

Some of the actions to be taken for protecting the computer systems are

- Firewall.
- Protection software.
- Does not consider unknown attachments.
- Don’t run unknown origin.
- Use hidden filename extent icon.
- Turnoff the system when not in use.
- Regulates backups of difficult data.

1.2.4 **Switching Networks**

Several services which are provided are: VLANs, QOS switching, physical address location, CSMA/CD, flow control, and framing network data packets.

**Physical Address and Switch**

Switch is an inter-connecting device commonly used for 16 or 24 ports. In other words, devices are connected to these ports. Basically the source machine sends a packet to switch then proceeds to its destination machine. In each comes to switch contains address in it, and the method of forward switching techniques. Each switch case can send packet based on destination MAC address. It follows:

- The receiving switch from any device, checks the address of MAC.
• It compares address of MAC with its destination MAC address from the corresponding table.

• If it is found the packet is out of port against the MAC address was not matched.

• In other way, the MAC address has generated the request of ARP.

**Working principles of ARP**

The ARP performs the following ways

• The sender machine generally generates the request of ARP packet with the address of machine; finally the switch can receive the SIP address from sender and receiver.

• All the incoming packets which are received from the respective MAC address to the switching center, if it is not found the switch can add and entry of visitor location register port with the address of MAC.

• A switch broadcast packets are also in the networks.

• Each network can receive the entire packet from the ERP receiver and compare with source IP address as well as the destination IP address.

• If the MAC address not found, the ARP request is generated and the MAC address is obtained from the contention window information.

• Sometimes MAC address matched with forward packets on the port number of the matched packets.
Using ARP table the host machine will receive MAC address and ARP replies.

1.2.5 Interface

The interface is the access point which attaching the process of communicate much as an embedded interface. The attached TCL process can also detached the ECL Process. This disconnection, termination and clean up links between the ECL and TCL processes. In typically the programmer wants to accept a specific application to be used through the remote and embedded interface, the code that needs a specific one or more another interfaces to associate with beginning and ending of the application.

In human computer interaction a well as computer program refers to text, audit information, graphical location of the program presents to the user to control sequences of user employs sub program (computer key stokes, movement of the mouse, the selection of touch screen).

Types of Interfaces

- Direct Manipulation Interface

  Direct manipulation interface allows user to manipulate the objects, according to least loosely to the physical medium or world.

- GUI

  Graphical User Interface (GUI) accepts input device such as keyboard, mouse, and graphical output on the monitor which are widely categorized by GUI design. Initially object oriented user interfaces and application oriented interfaces.
- **Web User Interfaces**

  Web user interfaces accepts input and output by the authenticated web pages are transmitted via internet and web browser program. The utilized implementation of java, Ajax, adobe flex, Microsoft.net or other similar technologies can provide separates program for clearing the unwanted data and to refresh the traditional html browser. The control panel which consists of web server, network computer using administrative web interfaces which are called control panels.

- **Touch Screen**

  Using finger stylish or touches to accept the display of related web pages or content used in a growing way of mobile resources and point of scale, self services machines etc.

- **Command Line Interfaces**

  The users provide the input by inserting a key stokes using command strings with the keyboard and finally the system provides output device (computer monitor) by providing the text or emails or graphical data. For the use of technically advanced computer users may utilize the areas of engineering, scientific environment and programmers system administration.

- **User Interface Using Touch**

  Using touch pad or touch screen it can display the combined input and output devices. It can replace other forms of output with suggestion methods in some simulators etc.
• **Other Types of User Interfaces**

Some of the other types of user interfaces are

- User interfaces using attentive
- Group Interfaces
- Agent Interfaces
- Mesh Interfaces
- Mouse Interfaces
- Artificial Intelligence Interfaces
- Apple Interfaces
- Multi screen Interfaces
- Command user Interfaces
- Object Programming Interfaces
- Reflexive user Interfaces
- Overload focused Interfaces
- Voice Interfaces
- Zero input and output Interfaces
- Zooming Interfaces

1.2.6 **Proxy Server**

A Computer is a proxy server which offers network service to create in direct connections of network computer services. Each connection to provide proxies (server), and then contribute files, connection, resources and other variety of servers. A proxy provides either by inter linking a specified
server or from a secondary storage device. In which the clients request or receipts response time may vary under different manner

**Proxies (Web)**

A basic application of web proxy is a cache. It describes nearly files, web pages and server (remote web server). It specifically allows Local area network users to access more easily and with more integrity. In which each receiver receives a request from a specified URL, it took or providing results of internal cache, if it returns the content quickly. In other words the remote location server fetch the related content, or returns requested to provide the content of cache in save, copy and etc,. A secondary storage device normally expired steps to clear that content from the secondary storage, accordingly their history of information (Integer with and related information). Two main simple steps are 1.Least Frequently Used 2.Least recently used. Specifically, Least recently used materials or documents. Likewise Least frequently used removes frequently documented. Proxies also provide the content of filtering for web page services. In some cases to attempt offence of block content (web) are implemented by proxies. Other services are recreation of web pages, specifically audience or specific reason, example re clear pages are mobile phone and PDA’s. Computer network operators are deploying intercept of system viruses and other content of remote location web.

There are websites which allows a user to access site. In generally, PHP or CGI implementing some related functionality where in frequently used to gain access to be blocked by concern proxies. Since there exit the hide of users personal IP address from the site, they access through the proxy, sometimes they used an anonymity of level.
Sorts of Proxies

- **Proxy of Transparency**

  Proxy of transparency provides original IP address via HTTP. In generally used for catch websites and have not effectively concentrate the anonymity of the users. The user transparency proxy will get around IP area. It terms of transparency it contains IP address existing, should not transparency in the terms of using specific configured to the user.

- **Proxy of Anonymity**

  Proxy of anonymity provides identity as server, does not provide any kind of real IP address. It may be configurable, reasonable and flexible for majority of the users.

**Higher Level Anonymity**

High level anonymity does not provide the identification of proxy servers and does not mean the real IP address

**Issues with Proxy**

In using proxy server every data forward to the service using HTTP server in the website location. It must passes periodically through the server proxy the beginning we can send or forward, most recently decrypted form. Therefore it demonstrated a malicious proxy server to store every users content forward to the proxy. It belongs to sign in procedure. In continuing, a proxy does not have repeated data about the original requested data. It can possibly abuse activities from the human eyes of the users peer points. However more traceability will be left out, which can be used or sponsored to trace out users functionaries. In such kind of policies, administrators and other
proxies are all unknown, the sender may fall victim to a wrong sense of security, because of details are out of site and control.

The ground level line of users proxy servers, integrity level of proxies are trusted to provide a clear policy to the owner. And the integrity of unknown server never uses proxy, if there is no way eventually to utilize server proxies. In basically private information could not pass through the proxy.

**Abusing Proxies**

An open proxy is a proxy which accepts IP address from the client side and make relevant link to internet resources. Abuse of open proxies is recently significant portion of electronic mail delivery. Spammers usually install open proxies on end to end users. It means system viruses designated for this reason. IRC (Internet relay chat) abuser also frequently used this technique.

In over viewing of that, system administrators have introduced a number of possible ways to refuse to open proxies. The ethical way of testing clients are controversial. In some experts view, the testing to be equal to an attacker scanning the client host.

**Anonymous Online**

Internet anonymous is a crucial and essential portion of internet privacy and the issues. In this anonymity, fundamentally the way of people can forward messages and contribute business values through the internet without revealing true identity. This formation may reveal controlled by the specific user. It includes original user’s information, following internet anonymity and extends up to beyond the user level. In this computer
information and location are to be maintained internet anonymity to functionalize the internet without giving any traceable information or web activities or personal information era.

Those who have concern about anonymity of discussion the risks to personal privacy; these are consigned in cookies about privacy risk. In these, cookies are texts sending to a corresponding browser or the page has been visited. Again the computer server can resend the particular web page quicker and accessing the page is easy. It contains related information about the sender, e.g. Preference, ID’s and sign in details of electronic shopping information. This may belong to cookies consideration and privacy risk by the internet users and it is disabled by computer owner to the web page.

This method may not allow unsigned users to express themselves freely without worrying about discovered data or traceable data (ridicules). In this important discussion, forums are especially involving personal topics or queries, in which the participating users cannot allow to admit who they are. Like it is used in medical forums, the patients are free to clarify medical related question of doctors and others, Even though the advocate also can maintain such essential transmitting information from the above.

The originality of the internet unsigned users that can be subjected to head discussion for years to come. Fortunately, existing avenues of such users take place to protect their personal identity, references and address. Finally, here the system will conclude the users need to remain cognizant of information on the internet access, including online profiles and editorial devices.
1.2.7 Disaster Recovery

In the perspective of disaster recovery, a part of contingency plan for the N-tier enterprises is to restore loss of data in the occurrence of system failure, natural disaster, fire and others. Regarding the causes of system critical situation cannot quit because quickly down time can translate immediately to advertise the loss of data to concern services. In fact, various companies experience does not recover from the financial impact. For that the application companies may not start as mission critical, but the years of grow a core application for concern business may be better based on the disaster recovery rule. That’s why every IT implementation must need to protect the plan to invest and prevent the business from the causality.

Methods of Disaster Recovery

To select the right disaster recovery approach, some important key contents are used for keeping mission critical:

Manual solutions – These solutions usually involve manual procedure (Recover time and sophisticated vary)

Constant Replication – It is basically following the method of progress open edge replication. It describes copies of information from one or more sites and provides failure recovery to keep constantly data available.

Configurable Process - It combines software and hardware solution with redundancy .It may be automated and configurable.
Many companies home ground solution to address their requirements to make the data recoveries through automation process. Consequently varying the result the solution may not affect the flow of transmission but the manual may not able to process based on user needs. As shown in Figure 1.5, the home ground solution data base backups must take artificial images to capture as much as possible.

With this method, the attention is given for the protection of user who needs to ask how much data to loss and how quickly can retrieve from the original spot. These are all the related factors for production backups. Lost transaction could mean lost of business, lost of dollars, exactly what are trying to clear or in other words home ground solution is not real time solution. But it provides data base policy insurance in the event of failure.

**Primary and Secondary Replications**

The goal is to stabilize down time in the event of error or critical situation by switch over the hot-standby server. In this method, builds a real time failover environment for open edge replication software. Here we can
choose automatically or database administrator initiates failover. In shortly it has the advantage of hot-standby database. If reporting users are picking up valuable resources on the production system, then it can offload them to hot-standby with replication plus and gain the benefits of production system.

Specifically, the open edge replication software sits on top level progress installation but there is no change of application needed, everything configured via the files replication should function. In summary, the databases are single point of failure and create major availability of the environment (Figure 1.6).

![Figure 1.6 Primary and secondary replication](image)

**Failover Clusters**

Open edge clusters provide an operating system, vendor system or both independent solutions for an automatic failover to the open edge database. Here needs to enterprise database and a license for the additional
servers. For software and hardware have redundancy but also need shared storage devices. With this open edge cluster for failover we need two independent nodes (servers) with the progress enterprise software. These environments connected to anyone common storage device. To finalize the environment need cluster management software from the globally certified vendors such as Microsoft, Sun, HP and IBM.

Open edge cluster provides the facility to eject machine failure point, database protecting access from the database server. In a cluster technique redundancy software and hardware are put in a point to enable failure. The most significant ways of clusters is to ease of use and ease of maintenance (Figure 1.7).

Figure 1.7 Clusters for open edge process
**High Availability Clusters**

When combining the technologies, elimination of failure points as possible due to replications, redundancy and software and hardware and databases. Using this process, it can control the failure and can help better achievement of entire goal. The above mentioned portfolio also delivers fast data replication management, tools analysis performance, managing visibility, and critical information assets.

### 1.3 RESEARCH MOTIVATION

Information Technology operations are a crucial aspect of most organizational operations. One of the main concerns is business continuity; companies rely on their information systems to run their operations. If a system becomes unavailable, company operations may be impaired or stopped completely. It is necessary to provide a reliable infrastructure for IT operations, in order to minimize any chance of disruption or disaster and to sustain the adequate performance of the systems.

These days, Information technology operations are facing various typical challenges. They are,

- Availability of Critical data at all times.
- Huge cost involved to recover the systems in case of disaster.
- Performance hindrances due to growth of historical data.
- Network Traffic Congestions.

This research focuses on the problem of web application performance and its impact over the organization.
1.4 THESIS ORGANIZATION

This thesis is organized as follows:

In **Chapter 1** the overview of the web application elements that are participating in the web architecture. Also, it contains of motivation research.

**Chapter 2** reviews the existing web application performance studies with their pros and cons. It discusses the various web application performance and their characteristics. Also, it contains the key challenges of web applications.

**Chapter 3** describes about the problem statement and research methodologies.

**Chapter 4** elaborates on fixing the network congestion problem by bypassing the load using F5-Load balancer and providing the reliable network security through NS-IDS.

**Chapter 5** details about the database server load and implementing the load balancing methodology.

**Chapter 6** explains accelerating the data transmission with security mechanism.

**Chapter 7** provides key issues related to web application.

**Chapter 8** exhibits the results that are obtained from the research to evaluate the measures of web application performance.
Chapter 9 presents the conclusion drawn in this thesis work along with the possible future scope of research directions which can be shown in this research work.