Chapter 7

SUMMARY, CONCLUSIONS, FINDINGS, SUGGESTIONS, RECOMMENDATIONS, LIMITATIONS AND IMPLEMENTATION

7.1 Summary:

1. From the case studies we have seen that many learning fields have not established the safeguard environment at their working place. It has been observed that very poor line of attack they have used to design the networking. Therefore there are many breaches in the networking. It is very important to understand that just by using networking security tools we cannot make sure of a secure situation. Inadequate design can lead to the vulnerability of the valuable data, to hardware and the softwares that are connected with the main computer.

Hence it is necessary for learning fields to take guidelines from the Information Technology professionals to design the safe network for their learning fields. From this we have proved that the proper use of the security tools is required to enforce the networking control in the educational institutions.

2. As it is observed that the main benefit of having the networking is to share the peripheral devices and the applications softwares. From the surveyed results it is seen that majority of the learning fields are using the old-versioned that is out-of-dated version softwares. And this becomes the entry point for the benchers to access in the networking. And they can easily destroy the valuable information of those educational fields. To reduce this factor it is suggested to have updated softwares in their main terminals and even on the workstations. We should never use the
plagiarized version of softwares as if pirated softwares are used then it will be like entry point for the hackers. So it is very essential to have regular updating of the application programmes which are installed in the servers and the workstations.

3. The another accessible point for the hackers to get into the networking of the learning fields are through the electronic mails. To reduce or to minimize this threat every user must use the anti-virus software to scan the electronic mails before opening it. Every computer should have the electronic mail security software installed in their computers. By doing this vulnerability of the electronic mails can be reduced at great extent.

So we conclude that it is very essential to make every employee of the learning field to understand that never open any electronic mails before scanning them to secure their valuable data.

4. The another vital factor is to have the strong network configuration to avoid the vulnerability. As the weak networking configuration becomes the plus point of the hackers to get access in the networking and play with their valuable data. Hence it becomes the first priority of the network manager and the IT professionals to design the network in such a way that there are many fissures in the design. To achieve this it is essential that every learning field must follow the documentations and the protocols for designing of the network architecture and must follow the course of action to have a secure networking situation for their working place.
5. Another point to take into consideration is the use of the external devices, USB and the flash drives. Every learning field should give the training to the employees that before using these kinds of the devices it is advisable to first scan the device and then only do any kind of actions like copy or delete the files from such external devices. It is compulsory that put the scan before use check box always clicked so that whenever the user is inserting such devices then the computer first will scan the device and the networking can be secured.

6. As it is surveyed that from many security tools the most commonly used security measures are the authentication, anti-virus softwares, firewalls etc. Therefore while using these security measures read out all the rubrics and the manual given with that security tool and then installed in the main server.

To just have the internal and the external firewalls with the default settings is not enough to secure your data it is essential that the learning filed should change the settings according to their requirements.

If one is using the anti-virus softwares then it is very important to keep the regular updation check box on so that on the regular basis your anti-virus softwares are getting updated which will help to safeguard your data from many threats.

Even it is observed that not only the technical threats are there for the data but also there are internal threats which can harm your valuable data.

7. The first category which I like to discuss is the employees of the learning fields. As he or she knows everything related with the security of the networking. Therefore they can easily alter the data of your institutions.
To reduce this internal threat it is compulsory to make the layered network security it means each employee should have the permissible and non-permissible rights according to their requirements. This will reduce the threat over the data at some extent.

8. Secondly I will like to talk on the password policy which is generally followed by the network analyst of the learning fields.

As almost all the computers are in the networking it is essential that each user of the learning filed should have their own login and the password. But it is seen that very poor policy of the password is kept which being easily tracked by the hackers.

To avoid this threat factor the learning filed must use the password generator software which can randomly generates the password for the users with the combinations of the letters, numbers and the special symbols.

Secondly it should make mandatory for every user to change their password on the regular basis.

9. Even natural disasters can damage your data. To avoid this we should take the backup of our data.

10. The last but not the least factor is to proper destroying of the data. It is seen that if the employees have not properly destroyed their statistics then the hackers can easily access these data. Hence is very important to properly destroy the valuable data so that there is no entry point for the hackers to do any amendments with the valuable data.
11. The last point to discuss is, if one finds that the computer which is in the network is under any of the above threats which are explained above then immediately remove the computer from the network and then clean up all the threats and then put it back in the network. By doing this the other computers and even your network remains safe.

12. Always use the licensed copy of the operating system and the application softwares which are required for the institutions. This will reduce the threats over the network and the data. If ones use the illegally copy of the operating system and the application softwares then the risk point of your networking and the data is increased at larger extent.

13. The very important threat on the local area networking which is basically seen in the almost every learning field is discussed below. If the hacker has installed the software called packer sniffer to produce the variety of numerous password then the criminal that is the hacker can easily get the root password and gets the access point in the networking.

So to eliminate or to block this threat it is suggested to have the challenge response password software installed in the main server which will simply ignore the password generated by the hacker’s computer.

It has been seen that from top ten targets the one of the target is the educational fields. Hence it is very important for the every learning field to be very precise in their networking design. There should not be any breaches while designing of the network structural design.
It is seen the most used attack techniques are the password hacking, account hacking, SQLi etc. Hence it is advisable that each learning field should use strong programming techniques and design setup so that they can stop the unauthorised users to do any kind of actions on the data.

Though lots of researches have been done on the networking and data security but still no one has still achieved the complete secure situation for their learning fields. Lots of revised security tools are designed by the companies but still there are some breaches in that the hackers are getting the chance to get inside and metamorphose with data.

Hence it is said that security and the privacy of the data is the procedure or the continuous development and it cannot be achieved in a day. It is process which we have to everyday to keep away the threats over the data. Here we have discussed several technical and the non-technical factors which can harm your valuable data and even the security measures by which we can safeguard our data from such threats till some extent.

So it is concluded that with the proper network security design and the configuration one can setup the secure network in their working place so that till some extent they can secure their data from the hackers. It is not possible to eliminate the threats over the data but at least we can reduce the threats over the data.
7.2 Conclusions

The researcher has given the most common network measures for the educational fields.

1. First every educational field should use the strong firewall and proxy server to keep away the unauthorised people to get into the network and manipulate the sensitive data.

2. In the present situation it becomes the need for every institution to have the internet facility. So it becomes very important for every institution to use the anti-virus softwares and the internet security softwares or packages to block the threats of the viruses and worms etc.

3. Due to the network security reasons in every institution each employee has his or her login and the password so that to access the information regarding their authority rights. So it is mandatory for the educational institutions to use strong policies for the password to secure their valuable information.

4. It is observed that many institutions have the wireless networking at their working place. And from the surveyed results it is clear that wireless networking is even more dangerous as compared to the wired networking. Hence it is advisable to use the robust password technique to secure their data.

5. To avoid the natural accidents it is advisable to use fire extinguishers near to the fire sensitive areas like the security rooms and the server rooms.
6. Every employee should know the value of the security of the data of their institutions hence is necessary to instruct them regarding the use of the networking security measures like how to use of the any external devices like flash drives etc., or their password policy etc.

7. As many institutions are using UNIX as the operating system so for them it is advisable to use the Ethereal open source network modus operandi to secure their data over the networking from the brechers.

8. The institutions can use the free and the trustworthy scanner which are available free on the internet to secure their valuable data and that is N-map security scanner. Another scanner which the institutions can use is the network vulnerability scanner which can help the educational fields to keep away the unauthorised people from their valuable information.

9. From many security tools the most commonly used techniques are the cryptography and the firewalls. Cryptography which secures the data and services for the educational fields. It is mainly based on the mathematical functions to encode and decode the messages. And therefore it is very difficult to crack the code and get the access for the brechers. Another technique which is widely used is the firewall. The firewall which is used secures the network traffic by studying the data packets and determining whether to send or block the packets depending upon the rules which are set by the educational fields.
10. The educational institutions should plan the security according to the present challenging requirements. It has been observed that hackers are no longer concentrating on the network layers now their target is on the application layer. Hence it become the first priority of the network expert to plan the security design in such a way that it will difficult for the hackers to get into the network.

11. Mostly it is found that the attacks are mainly due to the human errors. Hence it is very significant to train the employees of the educational fields so that the attacks can be reduced or can be prevented by just using the guidelines which are mentioned while purchasing the hardware or the software.

12. It is found that the anti-virus software is very useful to remove the malware. But is found that as the new malware is introduced by the virus programmers then it becomes little difficult for the software to detect that virus at remove that from the computer. Before it reorganized that virus that virus takes the complete control. And after that it becomes very difficult for the anti-virus software to remove that bug. Hence it is proved that regular updation of the softwares is very significant for every educational field to prevent the hackers from fiddling of the data.

13. Researchers have shown the recent development in the security areas to prevent the hackers to fiddle with your valuable data. Latest improvement is done both in the hardware and the software for the security of the network and the data. Biometric and the smartcard are the two most recent developments in the field of the security. They have reduced the growth of the breachers which fiddles with the
data. Biometric is used as the authentication mechanism as two individuals cannot have the same biometrics.

In case of the smartcard, it is issued to the each employee of the field and along with it a pin number is given to them which is consists of four numbers and the characters which are easy to remember by any of the employee.

When the employee enters at their working place, they have to insert the card and then they have to enter the pin number as the pin number which is given by the network experts only so the chances of the perfidy of the pin number is very low.

The widespread advantage of using the smartcard is it is less expensive and without the card there is no use of the pin number and vice versa.

Even it is observed that in terms of the software technology certain developments are there. The most useful advantage which seen is the neural networks for the face identification software.

From this the researcher have concluded that the networking security have to go forward to stop the threats in the imminent. From this it is ascertained that the proper use of the security tools can enforce that is improves the network security control in the educational fields.

Security is an endless game in which nobody can win or lose. It is like tail without the tale that is the attackers will come up with new hacking techniques and the network specialists will fine the way out from it.
7.3 Future work

The networking and the use of the internet will increase in the forthcoming years; this we say that from the current use of the networking and the internet use by the educational institutions. Hence even the threats and the risks will increase on the networking and the data of the every organisation. Hence it compulsory for every institution to understand the future trends, risks and the threats that are associated with the networking and the data. The security plan which are designed by the network manager for their educational fields need to be according to the today’s threat level and it need to be flexible according to need of the future.

7.4 Findings from the interpretation of data

It is seen that though the educational institutions are using the network security measures the data and the network is not safe.

1. There is requirement for the better network security measures so that they can give fully secure environment to the educational institutions.

2. The powerful network security measures make every organisation especially educational fields to work more confidently as they are assured that their data is safe on the network.

3. It is responsibility of the every organisation to secure their data from the unauthorized access.

4. One should use the various network security measures like firewall, authentication etc. to enforce the network security controls in the educational fields.
7.5 Suggestions for the effective implementation of security measures to enforce the network security

The ultimate responsibility for implementation of security measures falls on the organisation only. It is the responsibility of the network administrator to look after the entire network and safety of the delicate data. To secure a single computer is very easy but the challenges in front of the administrators are to secure the entire network against the unauthorised access. A significant amount of research has been done to resolve network security problem but it still remains to be a challenging due to increased difficulty and various threats peeping into the networks daily. A lot of techniques like firewalls, verification, anti-virus softwares etc. are being adopted but they are not result into a complete solution. As a result these tools and techniques proposed earlier may become out-of-date for solving network security problems at large. Hence it becomes the responsibility of the network managers to work more on these techniques to obtain the secure network environment.

7.6 Ways of Data security:

It is very important to have password policy in the organisation so that hackers cannot hack the password and reach to the sensitive information. To minimize the password cracking User-generated passwords has to be implemented in an organisation which follows a predictable pattern. This software randomly-generates the passwords and it is not easy to remember. Use a professional password-generating program which is available in the market. In addition to this train the users on how to maintain the password policy and give additional verification steps so that it becomes difficult for the hackers to crack the password.
Demolition of the sensitive data: Reports and catalogs may contain sensitive data hence it is very important to destroy them so that those data cannot be misused by the intruders. A data break can occur if data is not erased properly. Hence it is very important to destroy the sensitive data by using proper safety policy.

To summarize there are various threats to an organization’s information system and hence it is important to create a data security protection policy which can reduce both technical and non-technical threats.

7.7 Latest improvement in the network security measures

Preventing and detecting attacks that are caused over networks is probably the most interesting aspect of security. The problem will be solved as many researches on different kinds of vulnerability are being done by the network managers. One day people will run carefully written code on trustworthy platforms. It is found that firewalls will keep out the worst of the attacks if careful configuration management is done and intrusion detection will also help us to prevent the attacks.

With this security threats are also increasing. But it is seen that by using suitable security structure one day we will get a fully secure environment.

The next Generation networks which are the most flexible and enough to support the internet protocol version 6. They work as the checkpoints as it study and filter traffic for the threats and the malware. To order to protect the next generation network security devices should be based upon the high-scalable and easy to maintain platforms.

The IPV6 is the most likely network protocol used today by almost every organisation and even the educational fields. As the internet protocol version 4
cannot check the IPv6 traffic. Security protection is the part of the next generation networks via IP protocols as it can expose all the threats which are related with the internet. The most significantly, a basic component of the NGN concept is the network procedure. The NGN is the extensive model covering a range of network types both wired to wireless networking.

The smart card and biometric technology are the other methods which can be used to protect the data.

### 7.8 Certain Recommendations for further Research

1. Further research can be carried out in any other organisation like social web sites, commercial fields etc.

2. Further research can be carried out for more than 100 numbers of selected populations.

3. Further research can be carried out for any other area than the area taken in the present research.

4. Further research can be carried out can be carried for any other selected population than the selection taken in the present research.

5. Further research can be carried out for one specific security measures.
7.9 Limitation of the research

1. The research is limited to the one particular area that is Malad.

2. The research is limited only to the learning fields.

3. The research is having the limitations of numbers of selected populations.

7.10 Implementation of the Research

From the analysis of the research, it was revealed that there are certain holes regarding the data and the network security and hence there is a need to create the fully secure network environment.

Academic organizations are among the most targeted information systems in the world. Their extremely decentralized set-up makes it difficult to safeguard reliable security measures across their networks. Furthermore academic institutes have different departments with various users like faculty, staff members, learners, and scholars etc. who are accessing data from the network. The possibility and impact of threats and damage to the privacy, integrity and availability of the data have been higher. The educational institutes are aware that the security of their information assets like IT infrastructure, confidential records, faculty and students personal details etc. is their uppermost priority in terms of risk and even institutions stability and reputation. Very minute research work has been carried out in this field. This paper suggest to work more on the implementation of the Information Security System in academic institutes and make the system and network secure against the unauthorized users.
Network security is key question of the new generation of computing because various types of attacks are growing day by day. Creating a network is not a big subject for network administrators but protecting the entire network against the different types of attacks is a great issue.

There are various methods and tools are available nowadays for destroying the entire network. This paper mainly emphasizes on the network security measures and also some main issues that can affect entire network.

The need for networking is demand of the today’s world. This paper gives the complete details of the advantages of the networking and different forms of the networking and why there is the requirement of security measures in the networking. The need of the various network security measures to safe the information from the network attacks.

Researcher has made the efforts to find out the cause that even though the security measures are used still important data and information are getting hacked and misused by the hackers. So it is the time that each organization should start working more on how to minimize the risks factors.

1) It is further proved that the level of securing the sensitive data has been increased after collecting data from the staff members and the students of that particular college.

2) After discussion with the network expert it is seen that they have started working more on the security of the data over the network and became more alert regarding their security level.
3) It is further proved that the level of security is increased after the discussion.

4) After the survey every learning fields has started giving the training to all the employees of their place.

5) They have started using the genuine softwares for both application software and the operating systems.

7.11 Topics for the Further Research

1) The research can be carried in the latest technology in the hardware that is biometric and the smart card technology.

2) The research can be done on the software technology that is neural networks.

3) How security is affected in social websites or any other are except the educational fields.

6) How could be wireless and wired networks can be made more secure?

7) Future of the network security

8) Secure passwords are often very difficult to remember. Discuss the role of the password generating software and the security

9) How security algorithms are used in cyber security?

10) Role of different organizations for the protection of their sensitive data and the suggestions to acquire fully secure environment.

11) The cloud computing technique for safeguarding your sensitive data.
12) The latest technology of Smart Card.

13) The biometric technology to protect the network and the data.

14) A progress of Next Generation Network.

15) Controlling the computers through the image processing and the voice recognition.