Journal of Cyber Security
DOI:10.32604/jcs.2021.024136

Tech Science Press

Article

Awareness about the Online Security Threat and Ways to Secure the Youths

Yeshi Nidup[*]

Phuentsholing Higher Secondary School, Ministry of Education, Phuentsholing, Bhutan
[*]Corresponding Author: Yeshi Nidup. Email: nidupy1982@gmail.com

Received: 16 September 2021; Accepted: 24 September 2021

Abstract: This study aimed to find out the awareness about the online security threat and understanding of the preventive measures to secure the youths from online risks. For this, a quantitative method was applied and the survey questionnaire was instituted to collect the data randomly from the youths studying in class eleven and higher. A total of 264 youths, 147 female and 117 male responded to the survey questionnaire. The data was organized and analyzed using Excel data analysis tool package, interpreted and represented in the form of graphs with some explanations. The awareness about the online security threat was found to be good with 20 percent completely aware and 58 percent aware of it. The knowledge about the two-factor authentication was found to be quite poor. There are 20.4 percent who knows a little and 14.7 percent who do not know anything and 29.5 percent who are not sure about it. The use of cloud encryption, security and protection with firewalls is not so familiar amongst the youth. However, the use of strong passwords for their mobile and other gadgets were mostly applied by the youths. The youths were also found to be concerned with the software and the system in their mobile and other gadgets as they responded that they update it frequently.

Keywords: Cyber security; cybercrime; information

1 Introduction

Online security threat has become emerging and urgent issues across the globe. With the rapid development in the use of ICT and technologies, online security threat is increasing. There is online scam, hacking of websites, hacking of personal accounts of emails and various social media accounts. These have already caused a huge disruption to an individual, groups, offices, organizations, agencies, companies, governments and the countries. However, for all these threats, there are preventive measures to counteract in order to reduce the risk from the online security threats. But this is possible only if there is adesquate knowledge and awareness about the threats, its consequences and the ways to deal with the problems.

Bhutan is no exception from the online security threat. After the Internet service was provided in 1999 in the country, the number of Bhutanese using mobile, computers, laptops and social media kept rising steadily. Consequently, online security threat increased proportionally. This has alarmed the people and the government, owing to its complexity and the potential to cause a damage at greater magnitude. Bhutanese have been victimized with online scam, cheated by both friends and strangers, cyberbullying occurred, and people got involved in various illegal activities through social media resulting in imprisonment. Most importantly, there are large population of youth who use mobiles, computers, laptops and Internet. The risk of online security threat is very high for the youths as they are mostly online as compared to the adults. So, the youths are more vulnerable to online security threat.

There are several ways to prevent or to reduce the risk of online security threat, each one with specific prevention or protection mechanism. But the awareness and knowledge of an individual about the online security threats and preventive ways to deal with multiple threats will play a significant role in providing a safe online environment. How aware are the individuals and how much people know about the online security threat? How much does an individual know about the preventive measure? To understand the level of awareness and the knowledge of our youth about the online security threat and preventive measures will make huge difference in their life as they continue to live in the online world.

2 Scope of the Study

This study explored the level of awareness and knowledge of youths in Bhutan about the online security threats and preventive measures. This study did not conduct an in-depth study. Therefore, the findings from this study are limited only to the awareness of online security threat and the knowledge about some of the basic preventive measures. The findings will be based on the quantitative response provided by the participants which was too general.

3 Significance of the Study

This study explored the youth's awareness and knowledge about online security threat and some of the preventive measures. This enabled to establish some level of understanding about the youth's awareness and knowledge related to online security threat and preventive measures. From the findings, relevant agencies and organizations will be able to conduct a program or carry out advocacy program to educate the youths. This study will also indicate the need of further research on similar areas to gain in-depth knowledge and understanding.

4 Research Objectives

4.1 To explore the youth's awareness about the online security threat.

4.2 To explore the youth's knowledge about the online security threat.

4.3 To find out what kind of measures are applied by the youths to prevent from online security threat.

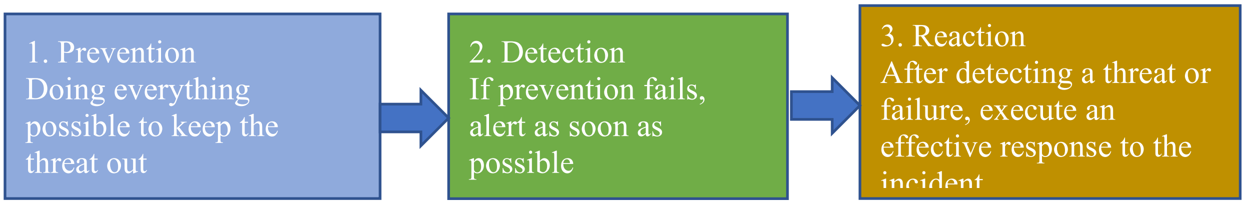
5 Literature Review

The rapid development of science and technology has revolutionized the digital world completely with new technologies. Along with the development of technologies, the challenges and issues associated with the use of technologies are increased manifold [1]. Moreover, with the multidimensional and complex setup of networks, there is high possibilities of cyber disruptions and cyber-attacks [2]. It is important to provide a safe environment which requires an in-depth understanding of the types and prevalence of online risks young Internet users face, as well as the options and solutions available in mitigating the risk [3]. Young adults nowadays arguably lack safety precautions when using smart devices such as mobile phone, laptop, desktop, tablet and many more. People update their everyday activity on social media which has become a source of privacy intrusion [4]. In the digital world, data can be sent and received with the click of a button but security and safety of a data is unpredictable. There is increase in online security threat due to more use of technologies and dependence on the Internet. Also, with the development of ICT and increase accessibility to the Internet, individuals are vulnerable to various types of threats [5].

The Internet threats are malicious software programs like spyware, adware, trojan horse, bots, viruses and worms which are set up on the system devoid of information or without any authorization [6]. Some of the online security threats are: virus threats-a program written to alter the system that a computer operates, hackers-a people who create computer security threats and malware, spyware threats-any program that monitors individuals online activities or installs programs without any consent for commercial gain or to extract personal information, phishing threats-masquerading as a trustworthy person or business to attempt and steal sensitive financial or personal information through false emails or instant messages, viral websites-websites that contains viruses that entice the users through email messages or links to visit the websites, adware and advertising trojan-these are installed with other programs that records a behavior on the Internet and also download other malicious software on the computer or mobile phones usually without users knowledge, unsecured wireless access points-if a wireless access point is not secured then anyone can connect to it and get an access to the internet and all the other, computers on the wireless network, bluesnarfing-using Bluetooth enabled devices to steal personal data, social engineering and Microsoft office document metadata-the hidden metadata with the details of who created it and who has worked on it can be viewed by using text editor in a word document [1]. Threats can be internal threats caused when someone has authorized access to the network with either an account on a server or physical access to the network whereas external threats can be related to individuals or organizations [5].

The use of Internet has caused an increased risk of online security threats associated with the integrity of our identities, our privacy and the security of our electronic communications, exposure to offensive and illegal content and behavior [7]. Smartphones or mobile phones have advanced features and capabilities just like the personal computers. Despite having all these features, smartphones have become an easy object for attackers. Sophisticated attacks are used against mobile phones which are more vulnerable than PCS due to lack of counter attack measures. Moreover, mobile phones have become sophisticated and multiple utility devices to store emails, passwords, banking details, online transactions activities and storage of information and important data [8]. To individual Internet users, cybersecurity risks can result in threats to confidential identity, identity as well as privacy [9]. It is deemed important and urgent for the youths to be aware of the consequences and challenges of cybersecurity and cybercrime because of higher recurrence of hacking assaults in the cyberspace [10].

Although there is greater awareness today, but there are still devices that connect to the Internet that have poor security measures or no security at all built-in because it was not a part of the design scope. There is evidence of lack of fundamental knowledge required for preventing from cyber threats [9]. Moreover, the idea that a device might be used for malicious act was not considered [11]. The safety of children and young people using the Internet and electronic technology has become a concern for parents, care givers, professionals, and the society [12]. It is crucial to understand security awareness among youth as they are heavy users of the Internet [4]. The Internet is an engaging medium for all children. Some youth deviance is an attempt to create excitement, interests, and group bonds when more conventional avenues for those rewards are not readily available [13]. The number of Internet users keep growing worldwide; it has become important to raise awareness on and highlight online risks and threats, to increase knowledge on issues that would enable Internet users to make the best of this medium, while being safe and secure. Internet has given greater access to the children, youth and adults which could expose young minds to harmful information that encourages hate speech or teachers and glorifies violence. This also exposes youth to certain risk like privacy threats, sexual harassment among other safety and security concerns which has the potential to cause damage to the well-being and development of children, youth and adults [14]. Besides, the children are generally aware of their behavior to stay safe online, but they often do not behave as required [15]. On the other hand, youths are sometimes inexperienced and naïve users, they become vulnerable to cyberbullying, cybercrime and breach of cyber security [16]. The lack of digital literacy and online safety measures exposes the youth to cyberbullying, cyber stalking, identity theft, sexual predation and other crimes associated with the use of Internet [17]. Also, the youths spend more time on the Internet, they can fall prey to malware which redirects their search results to fraudulent scam websites and pages [18]. The online security threats and cybersecurity readiness can be achieved by following the simple ways to secure the system as shown in Diagram 1 and adopting the five pillars of cybersecurity readiness as shown in Diagram 2.



1. Prevention
Doing everything possible to keep the threat out

2. Detection
If prevention fails, alert as soon as possible

3. Reaction
After detecting a threat or failure, execute an effective response to the incident

Diagram 1: How to secure the system from online security threat (Source: IJSRD, 2014)

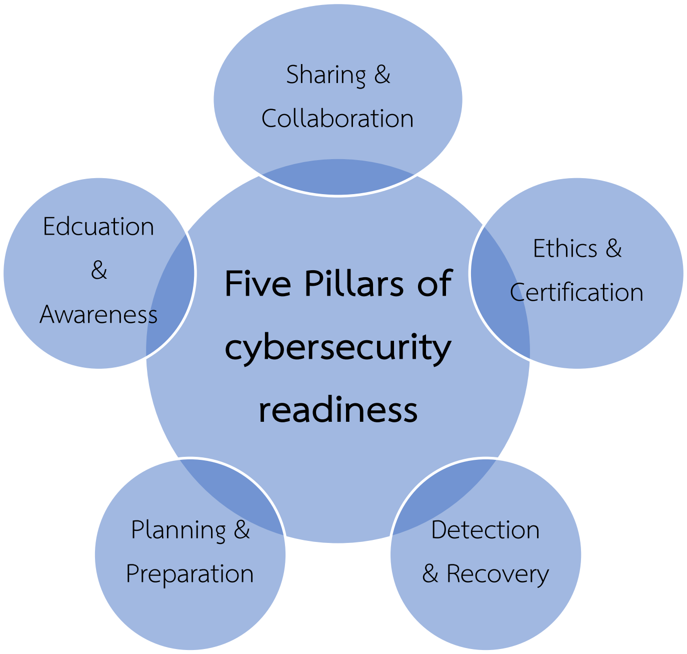


Diagram 2: Five Pillars of cybersecurity readiness (Source: ACS, 2016)

1. Education and Awareness: Cybersecurity talk has to be a part of everyday conversation, be it in formal or informal setting. The education must be provided at all times with regular updates to material as new threats arise.
2. Planning and Preparation: A good planning and preparation must be done in order to secure an individual or organizations from security threat. To do so, a good understanding of risk and threat associated with the use of all kinds of technology and Internet is important. Without adequate information and knowledge, it is impossible to plan and prepare cybersecurity readiness.
3. Detection and Recovery: When something goes wrong, it is always good to detect at early stage before things turn worst. If detections happen at early stage, there is possibilities to prevent the loss of data or damage of systems. A quick detection and recovery system are necessary.
4. Sharing and Collaboration: Collaboration is essential to mitigating and preventing of risks now and in the future. Moreover, sharing of the information, threats and risks that are thoroughly analyzed and studied must be shared with others to prevent or protect from the attacks.
5. Ethics and Certification: An individual or an organization must follow the ethics and fulfil the mandates under the purview of the certificates awarded. It is a moral responsibility of an individual or an organization to uphold the values of ethics and certification.

6 Methodology

A quantitative method was used for this study to reach out to a greater number of youths and also gain adequate knowledge and understanding of the youths and their awareness about online security and threat. Moreover, objective data is produced which is communicated with statistics and numbers. The data was collected quantitatively using survey questions as the participants were randomly chosen from different places. The questionnaire was designed with fifteen items using five-point Likert scale. The survey was done through the use of google form online. The snowball sampling was used to select the participants for the study. 117 male and 147 female, 264 youths in total studying in various classes ranging from class eleven to college students responded the survey questions.

7 Data Analysis

The data collected in the google form was converted to Excel sheet and further analysis was done using data analysis tool package in Excel. A descriptive analysis was done to analyze the data and graphs, pie charts and others were used to represent the findings and interpretations.

7.1 How aware are you about the danger of online security threat while using mobile, laptop, social media and the Internet?

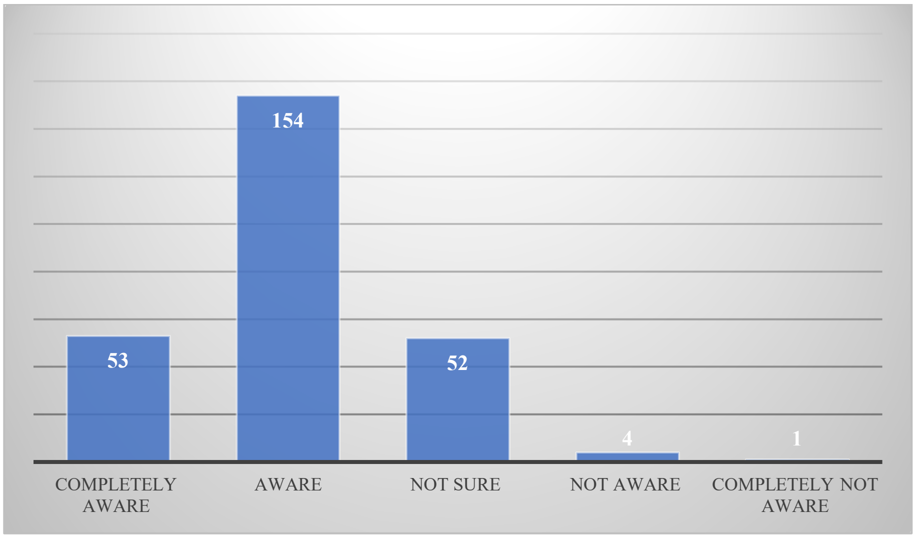


Figure 1: Awareness about the danger of online security threat

There are 20% (53) and 58.3% (154) youths who are completely aware and aware of the danger of online security threat while using mobile, laptop, social media and the Internet. There are also 19.6% (52) of the youths who are not sure of it.

Table 1: Awareness about the danger of online security threat

Mean	3.96
Standard Error	0.04
Standard Deviation	0.70
Confidence Level (95.0%)	0.08

The mean of 3.96 with the standard deviation of 0.70 indicate that the youths are aware of the danger of online security threat while using mobile, laptop, social media and the Internet. However, there is lack of complete awareness about the danger of online security threat.

7.2 How much do you know about two-factor authentication?

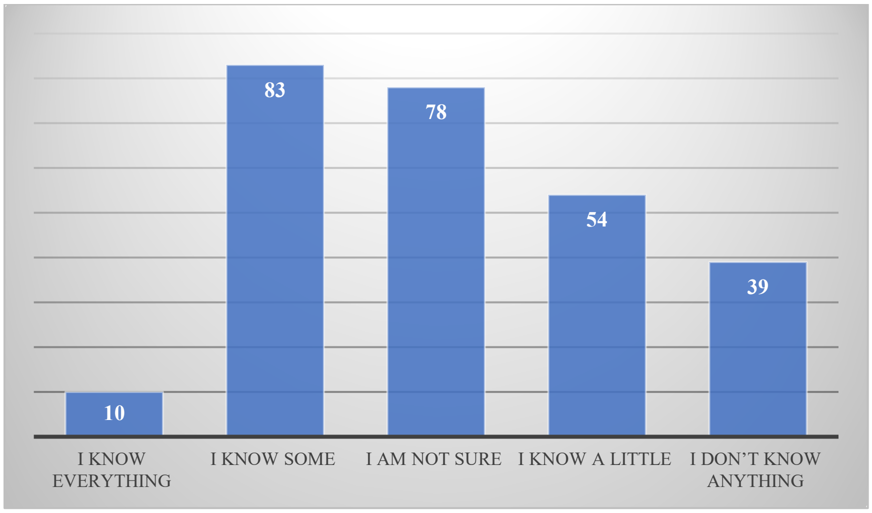


Figure 2: Two-factor authentication

There are only 3.8% (10) who knows everything, 31.4% (83) who knows some, 20.4% (54) who knows a little and 14.7% (39) who do not know anything and 29.5% (78) who are not sure about the two-factor authentication.

Table 2: Knowledge about two-factor authentication

Mean	2.89
Standard Error	0.07
Standard Deviation	1.12
Confidence Level (95.0%)	0.14

The mean of 2.89 with the standard deviation of 1.12 indicate that the youths know only a little about the two-factor authentication that is applied for online security and protection from threat.

7.3 All the password that I have created for mobile, emails, social media account and others have eight or more characters?

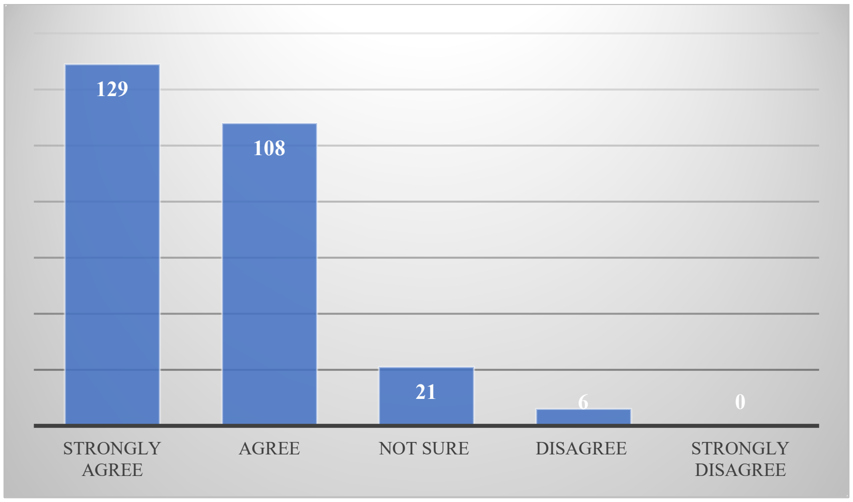


Figure 3: Password with eight or more characters

48.8% (129) strongly agreed and 40.9% (108) agreed that in all the passwords that they have created for mobiles, e-mails, social media account, and others have eight or more characters. Also, 7.9% (21) of the youths responded that they are not sure of it.

Table 3: Using password with eight or more characters

Mean	4.36
Standard Error	0.04
Standard Deviation	0.73
Confidence Level (95.0%)	0.09

The mean of 4.36 with the standard deviation of 0.04 indicate that the youths strongly agree that the password that they have created have eight or more characters. This shows that the passwords that they use are strong and safe as per the standard requirement for the safety and security.

7.4 In all the password that I use, there are more than 3 different types of characters (alphabets, numbers, symbols).

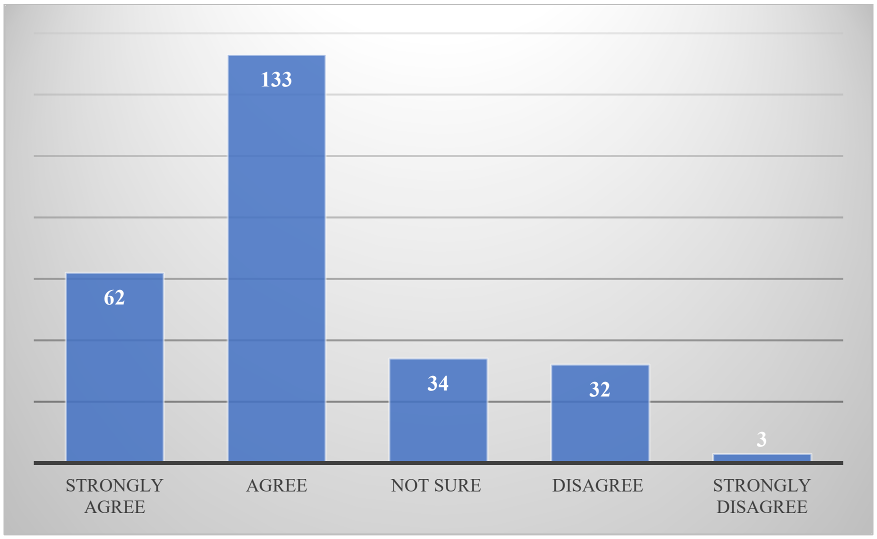


Figure 4: Password with more than three different types of characters

23.5% (62) strongly agree, 50.4% (133) agree, 12.9% (34) not sure, and 12.1% (32) disagree in all password that they use, there are more than three different types of characters (alphabets, numbers and symbols).

Table 4: Password with more than three different characters

Mean	3.82
Standard Error	0.05
Standard Deviation	0.96
Confidence Level (95.0%)	0.11

The youths agree that their passwords contain three or more different types of characters with the mean of 3.82 and 0.96 standard deviation. The higher standard deviation indicates that there is great variation in the response given by the youths about having different types of characters in the password.

7.5 I have saved information, data or any file in the cloud, using cloud encryption which will keep it safe from hackers.

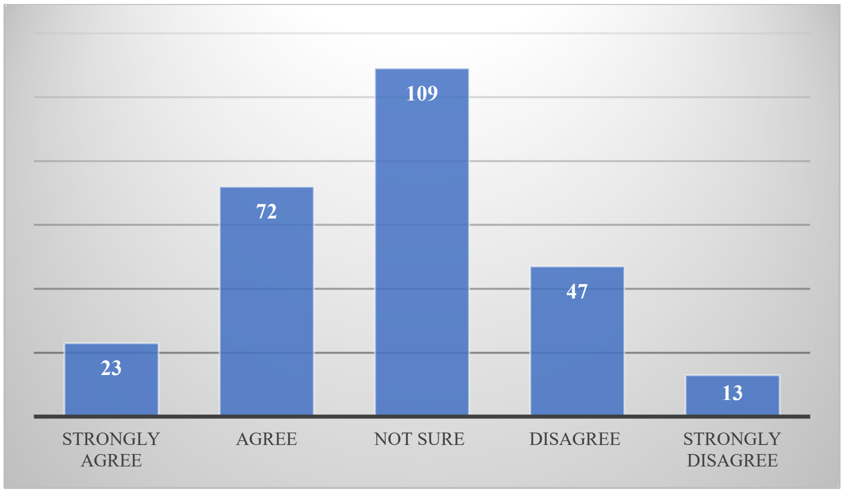


Figure 5: Use of cloud encryption

8.7% (23) strongly agree, 27.3% (72) agree, 41.3% (109) Not Sure, 12.1% (32) Disagree and 1.1% (3) Strongly Disagree that they have used information, date or any file in the cloud, using cloud encryption which will keep it safe from hackers.

Table 5: Use of cloud encryption

Mean	3.17
Standard Error	0.06
Standard Deviation	0.99
Confidence Level (95.0%)	0.12

The use of cloud encryption to save information, data and files by the youths are not so common. The mean of 3.17 with the standard deviation of 0.06 indicate this clearly.

7.6 How aware are you about the security and protection of your computers, mobiles, iPads & others with firewalls?

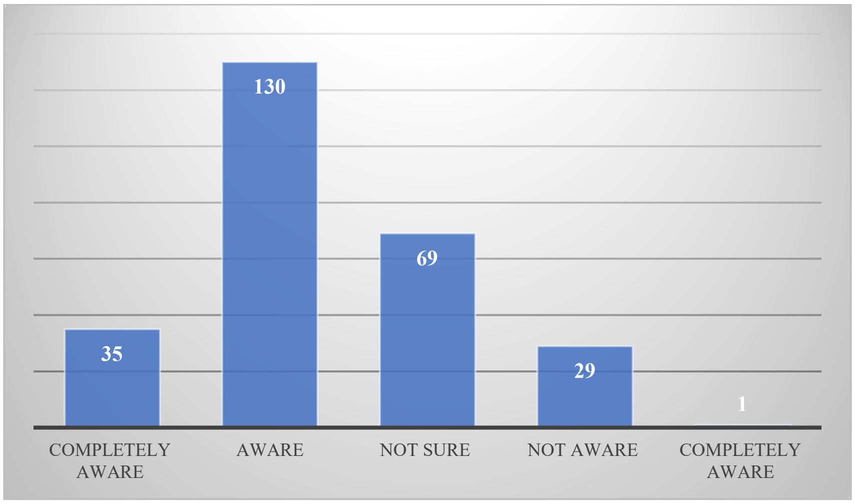


Figure 6: Awareness about the use of firewalls to protect the gadgets

13.3% (35) Completely aware, 49.2% (130) Aware, 26.1% (69) Not Sure, and Not Aware 10.9% (29) about the security and protection of your computers, mobiles, iPads and others with firewalls.

Table 6: Awareness about the use of firewalls to protect the gadgets

Mean	3.64
Standard Error	0.05
Standard Deviation	0.86
Confidence Level (95.0%)	0.10

The youths are aware about the use of firewalls to protect the gadgets as indicated by the mean of 3.64 with the standard deviation of 0.05. There are some who are completely aware and some who are not sure or not aware as indicated by the standard deviation.

7.7 In my mobile, laptops, iPad, Tablets, or other social media, I have used firewalls.

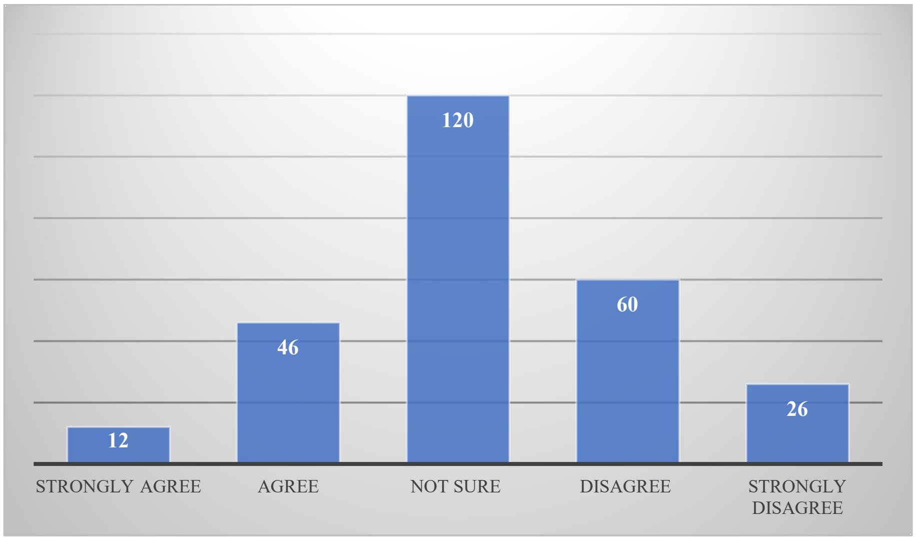


Figure 7: Number of youths who use firewalls

4.5% (12) Strongly Agree, 17.4% (46) Agree, 45.5% (120) Not Sure, 22.7% (60) Disagree and 9.8% (26) Strongly Disagree that they have used firewalls in their mobile, laptops, iPad, Tablets, or other social media.

Table 7: Youths who use firewalls

Mean	2.85
Standard Error	0.06
Standard Deviation	0.97
Confidence Level (95.0%)	0.12

The use of firewalls in the mobile, laptops, iPad, Tablets and Social Media sites is not very common amongst the youth. Majority of the youths have indicated that they are not sure about the use of firewalls and only few strongly agree and many who either disagree or strongly disagree as represented with the mean of 2.85 and standard deviation of 0.97.

7.8 I have installed Ad-blocker in my mobile, laptop or other gadgets which will help to prevent ads and other malicious tracers.

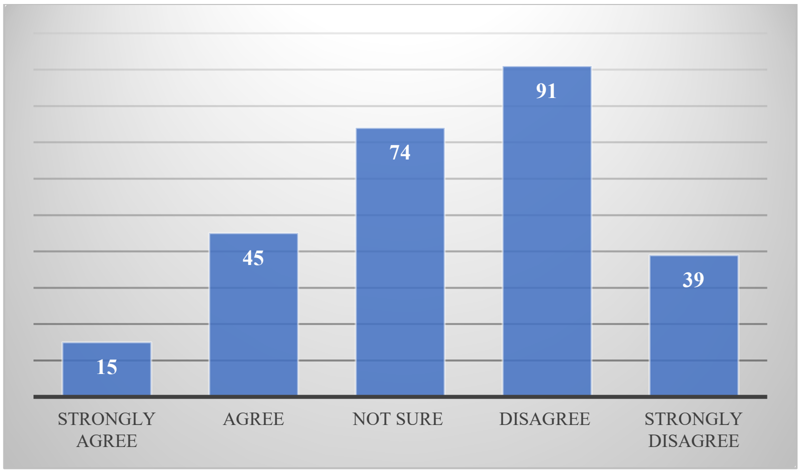


Figure 8: Use of Adblocker

5.7% (15) Strongly Agree, 17% (45) Agree, 28% (74) Not Sure, 34.4% (91) Disagree and 14.8% (39) Strongly Disagree that they have installed Ad-blocker in their mobile, laptop or other gadgets which will help to prevent ads and other malicious tracers.

Table 8: Use of Adblocker

Mean	2.63
Standard Error	0.07
Standard Deviation	1.10
Confidence Level (95.0%)	0.13

The youths disagree, strongly disagree or they are not sure about the installation of ad-blocker in their mobile, laptops, and other gadgets to help to prevent ads and other malicious tracers with the mean of 2.63 and standard deviation of 1.10.

7.9 I have used network intrusion prevention and detection software which can help to determine when someone has illegally entered my network or tried to access my accounts, files and folders.

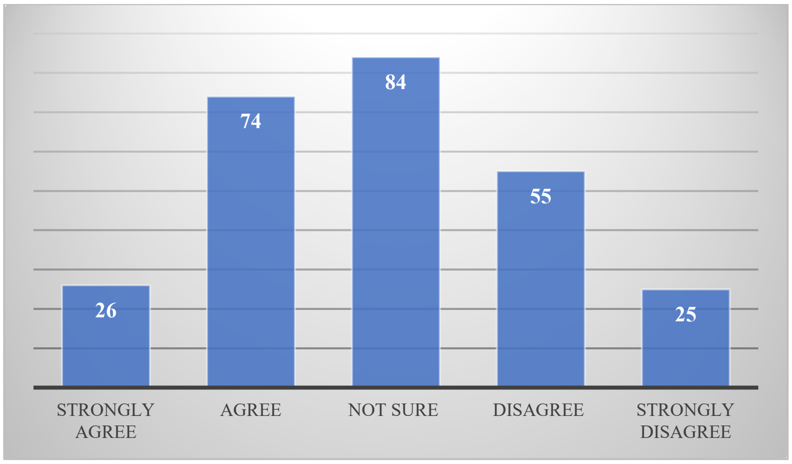


Figure 9: Use of network intrusion prevention and detection software

9.8% (26) Strongly Agree, 28% (74) Agree, 31.8% (84) Not Sure, 20.8% (55) Disagree and 9.5% (25) Disagree that they have used network intrusion prevention and detection software which help to determine when someone has illegally entered their network or tried to access their accounts, files and folders.

Table 9: Use of network intrusion prevention and detection software

Mean	3.08
Standard Error	0.07
Standard Deviation	1.12
Confidence Level (95.0%)	0.14

The mean of 3.08 indicate that the youths are not sure if they have used network intrusion prevention and detection software to determine when someone has illegally entered their network or tried to access account, files and folders. However, considering the standard deviation of 1.12, there are almost equal number of youths who agree or disagree about the use of network intrusion prevention and detection software.

7.10 I update the systems and software's in my mobile and laptop frequently.

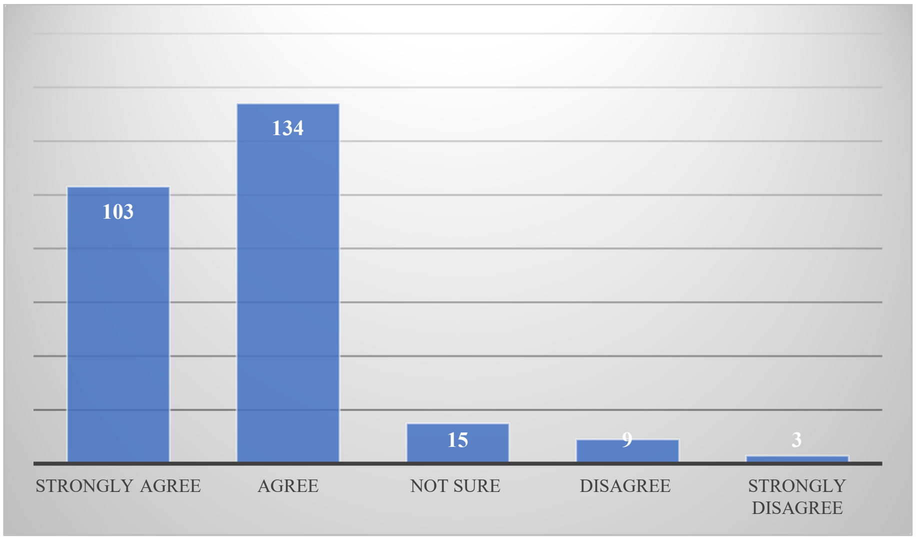


Figure 10: Update systems and software

39% (103) Strongly Agree, 50.8% (134) Agree, 5.7% (15) Not Sure, 3.4% (9) Disagree and 1.1% (3) Strongly Disagree that they update the systems and software's in their mobile and laptop frequently.

Table 10: Update systems and software

Mean	4.22
Standard Error	0.05
Standard Deviation	0.81
Confidence Level (95.0%)	0.10

The youths agree that they keep updating the software and systems in their mobile and laptops as indicated by the mean of 4.22 with standard deviation of 0.81. However, there are also few youths who do not update their systems and software.

7.11 I have encrypted and locked down all the data that is there in my mobile or laptop.

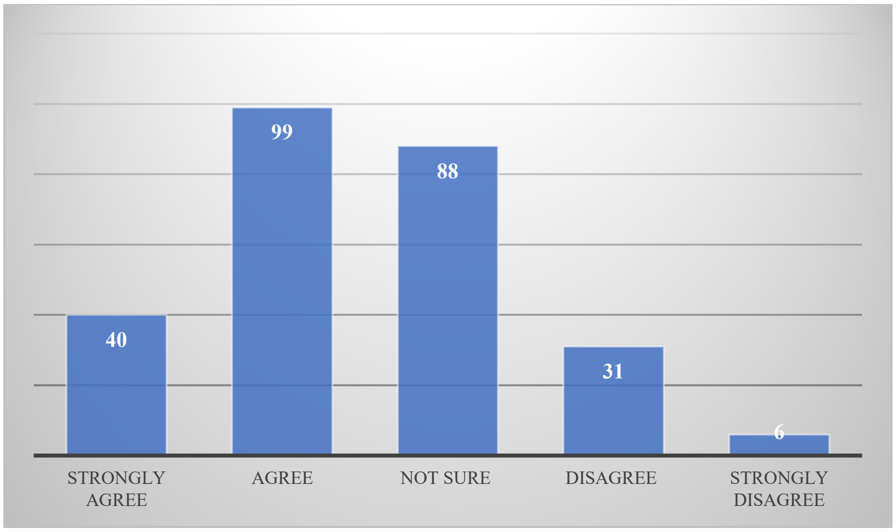


Figure 11: Encryption and locking of data

15.2% (40) Strongly Agree, 37.5% (99) Agree, 33.3% (88) Not Sure, 11.7% (31) Disagree and 2.3% (6) Strongly Disagree that they have encrypted and locked down all the data that is there in their mobile or laptop.

Table 11: Encryption and locking data

Mean	3.52
Standard Error	0.06
Standard Deviation	0.96
Confidence Level (95.0%)	0.12

The youths agree that they have encrypted and locked down all the data that is there in their mobile or laptop as represented by the mean of 3.52 and the standard deviation of 0.96.

7.12 I monitor my network and see what is coming into my network and what is going out of it.

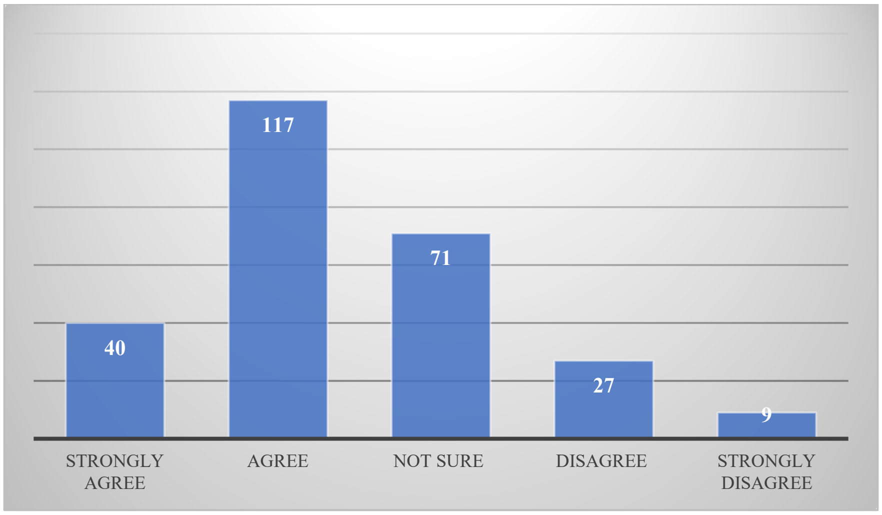


Figure 12: Monitoring network

15.2% (40) Strongly Agree, 44.3% (117) Agree, 26.9% (71) Not Sure, 10.2% (27) Disagree and 3.4% (9) Strongly Disagree that they monitor their network and see what is coming into their network and what is going out of it.

Table 12: Monitoring network

Mean	3.58
Standard Error	0.06
Standard Deviation	0.97
Confidence Level (95.0%)	0.12

The youths agree that they monitor their network and see what is coming into their network and what is going out of it as indicated by mean of 3.58 and standard deviation of 0.97.

8 Findings and Discussion

8.1 Awareness about the Danger of Online Security Threat

The awareness about the danger of online security threat pertaining to the use of mobile, laptop, social media and the Internet is good. There are 20% (53) who are completely aware and 58.3% (154) youths who are aware of the danger of online security threat while using mobile, laptop, social media and the Internet. There are also 19.6% (52) of the youths who are not sure of it which is a concern. This finding is in concoction with reference to [4] which stated that young adults today lack safety precautions when using smart devices such as mobile phone, laptop, desktop, tablet and many more.

8.2 Two-Factor Authentication

The knowledge about the two-factor authentication is quite poor. There are only 3.8% (10) who knows everything and 31.4% (83) who knows some about it. On the other hand, there are 20.4% (54) who knows a little and 14.7% (39) who do not know anything and 29.5% (78) who are not sure about it. This is a big concern since there are large number who do not have adequate knowledge about two-factor authentication. Due to this lack of knowledge, the cybersecurity risk can result in threats to confidential identity, identity as well as privacy to individual Internet users as mentioned in reference [9].

8.3 Password Characters

The youths have created and used strong password because 48.8% (129) strongly agreed and 40.9% (108) agreed that in all the passwords that they have created for mobiles, e-mails, social media account, and others have eight or more characters. There are only 7.9% (21) of the youths who responded that they are not sure of it. Moreover, there are 23.5% (62) youths who strongly agree, 50.4% (133) agree, 12.9% (34) not sure, and 12.1% (32) disagree that there are more than three different types of characters (alphabets, numbers and symbols) in all the passwords that they use. The use of strong password is one measure to mitigate online threats. The findings from this indicate that youths have better understanding about the need of strong passwords because they have created a password that contain more than eight characters. This is one good safety measures that the youths have followed.

8.4 Use of Cloud Encryption

There are 8.7% (23) youths who strongly agree, 27.3% (72) agree, 41.3% (109) Not Sure, 12.1% (32) Disagree and 1.1% (3) Strongly Disagree that they have used information, date or any file in the cloud, using cloud encryption which will keep it safe from hackers. This has become important because if the unauthorized user gets access to data, the intruder will not be able to decrypt it. Thus, cloud encryption will provide better security [19].

8.5 Security and Protection with Firewalls

A firewall system is necessary to implement and enforce access control between two networks, which usually guard an internal private network and from external factors that may intrude privacy and security by allowing specific forms of traffic to flow between them [20]. There are 13.3% (35) youths who are completely aware, and 49.2% (130) are aware about the security and protection of their computers, mobiles, iPads and others with firewalls. The findings indicate that the youths have some level of awareness about the use of firewalls for the security and protection. However, there are 26.1% (69) of the youths who are not sure, and 10.9% (29) who are not aware about the firewall protection system.

Moreover, there are only few students who have used firewalls in their mobile, laptops, iPad, Tablets or other social media as there were only 4.5% (12) who strongly agreed and 17.4% (46) who agreed. It is further confirmed since 45.5% (120) of the youths were not sure, 22.7% (60) disagreed and 9.8% (26) strongly disagreed that they have used firewalls in their mobile, laptops, iPad, Tablets, or other social media.

8.6 Ad-blocker

The use of Ad-blocker is uncommon amongst the youth because there were only 5.7% (15) of them who strongly agreed, and 17% (45) of them who agreed that they have installed Ad-blocker in their mobile, laptop or other gadgets. On the other hand, there were 77.2% (204) of them who were not sure, disagreed and strongly disagreed that they have installed Ad-blocker in their gadgets. This findings indicate that the youths are more likely to face problems in preventing ads and other malicious tracers.

8.7 Encryption and Lockdown

The encryption and locking down of data are deemed important for safety and security reasons by the youth. 15.2% (40) of them strongly agreed and 37.5% (99) agreed that they have encrypted and locked down their data in their laptop or mobile. However, there are also many of the youths who have not encrypted and lockdown the data. 33.3% (88) of them were not sure, 11.7% (31) of them disagreed and 2.3% (6) of them strongly disagreed that they have encrypted and locked down all the data that is there in their mobile or laptop.

8.8 Use of Software and Monitoring Network

The findings from this study shows that there is proper monitoring of their network and also check what is coming into their network and going out of it. 15.2% (40) of the youths have strongly agreed and 44.3% (117) agreed that they monitored their network. The findings also show that there are 26.9% (71) of the youth who are not sure, 10.2% (27) who disagreed and 3.4% (9) who strongly disagreed that they monitor their network and see what is coming into their network and what is going out of it.

There were only 37.9% (100) youths who strongly agreed and 28% (74) who agreed that they have used network intrusion prevention and detection software. 62.1% (164) of the youths were not sure, disagreed and strongly disagreed that they have used network intrusion prevention and detection software which help to determine when someone has illegally entered their network or tried to access their accounts, files and folders.

8.9 Software and System Updates

89.8% (237) youths have strongly agreed and agreed that they update both the systems and software in their mobile and laptop frequently. There were few of them about 5.7% (15) who were not sure, 3.4% (9) who disagreed and 1.1% (3) who strongly disagreed that they update the systems and software's in their mobile and laptop frequently. The findings from this shows that youths are more concerned about the system and software in their mobile and laptops as they seem to be updating frequently.

9 Conclusion

The online security threat is a big concern for everyone; it is even more risky for the youths as they are online most of the time. Moreover, most of the youths are not aware about the security threat and risk associated with the use of Internet and gadgets. Although there are measures that can be taken to mitigate various kinds of threats, if the youths are not aware of these measures available, they are highly vulnerable. However, the use of strong passwords and password characters more than three types are known and used by the youths. This serves as a gateway to prevent from the external threats. Moreover, one of the findings from this study indicated that the youths keep their mobile and other gadgets updated with the latest systems and the software. This is very important for the safety of the gadgets and the users as well. The awareness level is good for the use of firewalls for the protection and security. But the youths who have actually used the firewalls for the protection and security of their mobiles and other gadgets are very less as indicated in the findings. So, just being aware is not going to solve any issues related to risk and security threat if it is not applied.

The awareness and the knowledge about storage and keeping data safe is a concern since most of the youths are not aware and do not have adequate knowledge. There are only some youths who have encrypted and lockdown their data in their mobile or in the social media accounts. The monitoring of the network and use of network intrusion and detection software is not so popular amongst the youth. This may be a concern for the security threat or risks associated with the use of Internet, mobile and other gadgets. The youths must be adequately educated about the security threats and risk to provide a safe online environment. Otherwise, the youths will continue using the Internet and the gadgets exposing themselves to various online threats and risks.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Bhatia and R. Sehrawat, “Types of security threats and prevention,” *International Journal for Scientific Research & Development*, vol. 2, no. 8, pp. 281–283, 2014.

[2] A. *Mukherjee*, *Network Security Strategies, Protect Your Network and Enterprise Against Advanced Cybersecurity Attacks and Threats*, 1st ed. Birmingham: Packt Publishing, Ltd., Livery Place, 2020.

[3] A. Farrukh, R. Sadwick and J. Villasenor, *Youth Internet Safety: Risks, Responses, and Research Recommendations*. Centre for Technology Innovation at Brookings, 2014.

[4] S. Z. Omar, K. Kovalan and J. Bolong, “Information security awareness among youth in Klang Valley: A focus group discussion,” *International Journal of Academic Research in Business & Social Sciences*, vol. 10, no. 16, pp. 193–205, 2020.

[5] M. Jouini, L. B. Arfa Rabai and A. B. Aissa, “Classification of security threats in information systems,” *Procedia Computer Science*, vol. 32, no. 2014, pp. 489–496, 2014.

[6] S. Bhola, S. Kaur and G. Kumar, “Internet threats and prevention–A brief review,” *International Journal of Computer Applications*, pp. 13–17, 2015.

[7] Common Wealth of Australia, *Protecting Yourself Online*, 2nd edition. Australian Government, 2011.

[8] A. Sundaram, “Understanding and protecting yourself against threats in the Internet,” *Asian Social Science*, vol. 13, no. 12, pp. 201–226, 2017.

[9] P. Mai and A. Tick, “Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam,” *Acta Polytechnica*, vol. 18, no. 8, pp. 67–89, 2021.

[10] T. Alharbi and A. Tassaddiq, “Assessment of cybersecurity awareness among students of Majmaah University,” *Big Data and Cognitive Computing*, vol. 5, no. 23, 2021.

[11] Australian Computer Society, *Cybersecurity-Threats Challenges Opportunities*. ACS, 2016.

[12] National Children Bureau, *Keeping Children and Young People Safe Online: An e-Safety Strategy and Three-Year Action Plan for Northern Ireland 2019–2022*. Northern Ireland Executives, 2019.

[13] D. Finkelhor, *The Internet, Youth Safety and the Problem of "Juvenoia"*. University of New Hampshire, Crimes Against Children Research Centre, 2011.

[14] N. Alsherif, *University Youth and Online Safety in Egypt: Use and Trust*, M.S. thesis. The American University in Cairo, School of Global Affairs and Public Policy, 2015.

[15] T. Spielhofer, *Children's Online Risks and Safety: A Review of the Available Evidence*. United Kingdom Council for Child Internet Safety, 2010.

[16] D. Finkelhor, K. Walsh, L. Jones, K. Mitchell and A. Collier, "Youth Internet safety education: Aligning programs with the evidence base," *Trauma, Violence & Abuse*, vol. 1, no. 15, pp. 1–15, 2020.

[17] Child Rights and You (CRY), *Online Safety and Internet Addiction (A Study Conducted Amongst Adolescents in Delhi-NCR*, New Delhi, 2020.

[18] V. Sithira and Y. Nguwi, "A study on the adolescent online security issues," *International Journal of Multidisciplinary and Current Research*, vol. 2, no. 2014, pp. 596–601, 2014.

[19] S. Singla and J. Singh, "Cloud data security using authentication and encryption technique," *Global Journal of Computer Science and Technology Cloud and Distributed*, vol. 13, no. 3, pp. 31–35, 2013.

[20] T. Chown, J. Read and D. DeRoure, *The Use of Firewalls in an Academic Environment (JTAP-631)*. Department of Electronics and Computer Science, University of Southampton, 2000.