Original Article

A Study On Trojan Associated With Cyberbullying

Siddharth Kumar Bansal[1*]

[1*]MSc. Student, Department of Forensic Science, Chandigarh University, Mohali, Punjab, India

***Corresponding Author:-** Siddharth Kumar Bansal

*MSc. Student, Department of Forensic Science, Chandigarh University, Mohali, Punjab, India
DOI:10.47750/pnr.2023.14.S01.163

Abstract

This research is based on trojan which takes place when the cyber attackers hack the system of the computers to steal the necessary and confidential data from the computers for doing the misuse of it. The website phishing issue like the malware as well as hacking that can create to the leakage as well as the distortion of the confidential data. Lots of examples are present which provides the proper illustration. Such as deteriorating condition of India focusing on the improvements of the cyber world. This complete research is diverting the attention towards the spreading, creation and the malware processing which are related to the cyberbullying. The world of digitalization also leads to people and services which are becoming more interconnected digitally through the use of IoT in a society. The main terms of this complete research are the points which are represented in it like the trojan attack, cyberbullying, complex terms of the cyberbullying, prevention of the cyberbullying, how the trojan relates with the cyberbullying, methodology used for conducting the research, causes of the trojan attacks, prevention form the virus, antivirus that can help to prevent from the trojan attacks, uses of the blockchain, risks related to the blockchain, prevention form the attacks while utilising the blockchain, etc. are illustrated in this research of trojan associated cyberbullying.

According to National Law School of India report (2022), it has been stated that Malware like Trojan was developed along with personal computers, the first Trojan is theorized in the year the 1980s and it was developed in the year 1990. It is the name of the virus on a computer that is having the property of camouflage among the forms of regular software which can be games, utilities as well as programs, or an anti-virus. Malware creates the issues like destroying the processor's background system, deleting the important information of hardware as well as corrupting or contaminating the files of the system. Cyberbullying can be stated as the umbrella of various kinds of bullying activities that are more severe than others. In this matter the terms go beyond mistreating, calling, or making fun of other people. It also involves manifested in several types of dangerous forms which involve no limited harassment, exclusions, impersonations, outing, trickery as well as flaming.

The Malware can reach the computers through infected attachments, contaminated messages, or by the means of bogus web portals. Antivirus can protect the system from the attack of trojans such as Emsisoft Emergency Kit and Malwarebytes. The blockchain is an innovation that was created by fintech, it received a lot of attention since it gets originated as technology in enabling Bitcoins which are based on online transactions. The technology of blockchain is acknowledged by the advantages of recording events and transactions. Several people believe that the blockchain is quite similar to the internet which revolutionizes how organization and people like to manage transactions as well as assets. The technology of blockchain comprises two specific kinds of activities which are record hacking and double-spending.

1.1. INTRODUCTION

Trojan takes place when the cyber attackers hack the system of the computers to steal the necessary and confidential data from the computers for doing the misuse of it. The website phishing issue like the malware as well as hacking that can create to the leakage as well as the distortion of the confidential data. Lots of examples are present which provides the proper illustration. Such as deteriorating condition of India focusing on the improvements of the cyber world. This complete research is diverting the attention towards the spreading, creation and the malware processing which are related to the cyberbullying. The world of digitalization also leads to people and services which are becoming more interconnected digitally through the use of IoT in a society. The main terms of this complete research are the points which are represented in it like the trojan attack, cyberbullying, complex terms of the cyberbullying, prevention of the cyberbullying, how the trojan relates with the cyberbullying, methodology used for conducting the research, causes of the trojan attacks, prevention form the virus, antivirus that can help to prevent from the trojan attacks, uses of the blockchain, risks related to the blockchain, prevention form the attacks while utilising the blockchain, etc. are illustrated in this research of trojan associated cyberbullying.

Cyber threats can be divided into two main types: cybercrime, which occurs against an individual, business, etc., and cyber warfare, which occurs against a state. Cyberbullying can occur by directly targeting computers and viruses, or by using Denial of Service attacks, which are attempts to make a network or computer inaccessible to intended users. Software called malware is used to gain access to a private computer, collect sensitive information, or disrupt computer operations. Cyberbullying is drastically increasing as more and more users, and not just teenagers, become victims of this type of bullying. Cyberbullying issues are sad because a system that facilitates the flow of information and communication turns into a dangerous "site". Therefore, the internet can turn out to be dangerous if one is not aware of its functioning and security as a whole. People mostly support the idea that cyberbullying, along with regular bullying, is an important

reason for many social, anxious and depressed. Government and citizens alike should raise awareness among people to update their network and system security settings and use proper antivirus to keep their system and network settings free of malware and viruses.

(Image Source adapted from [19])

In this research study, the trojan virus or malware is going to be introduced which is related to cyberbullying. The trojan horse is the computer virus which utilize the various platforms like the computer games for destroying the important files from the system and stealing the useful data. When it gets runs within the computer, it creates the issues such as destroying the processors of the background system, deleting the data of hardware as well as corrupting the system allocation files. Cyberbullying is going to be highlighted that utilizes digital technology, it takes place through the use of social media platforms, gaming platforms, messaging platforms as well as mobile phones. It comprises repeated behavior, angering the person which is targeted as well as aiming at scaring. Cyberbullying is going to be illustrated in this research. Sending abusive or hurtful messages, videos, and images by the use of messaging platforms, spreading fake news or embarrassing post of a person on social media as well as impersonating an individual as well as sending fake messages to other people on behalf of that person by using the fake accounts are going to be presented on behalf of representing the concept of cyberbullying employing this research. Cyberbullying always leaves digital footprints, it creates useful records which can be utilized as evidence in support to stop the bullying. The combination of trojan and cyberbullying is going to be presented by the results of attacks which are related to trojan antivirus, corrupting the software of the user by using the trojan virus to create data theft for doing the misuse.

1.2. LITERATURE REVIEW

1.2.1. Trojan attack

According to [1], Malware like Trojan was developed along with personal computers, the first Trojan is theorized in the year the 1980s and it was developed in the year 1990. The development of Malware is kept pace along with the progressively sophisticated detection of Malware as well as the prevention of software. It is the name of the virus on a computer that is having the property of camouflage among the forms of regular software which can be games, utilities as well as programs, or an anti-virus. At the time of functioning in the computer, this malware creates the issues like destroying the processor's background system, deleting the important information of hardware as well as corrupting or contaminating the files of the system.

The **working of the trojan malware** is presented in the figure below: -

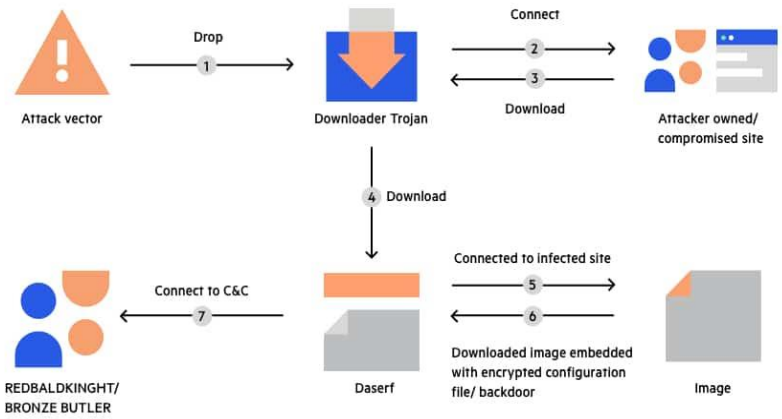

Figure-2 Working of Trojan Horse
(Source adapted from [17])

1.2.2. Cyberbullying

As per [2], Cyberbullying can be stated as the umbrella of various kinds of bullying activities in which some are more severe than others. In this matter the terms go beyond mistreating, calling, or making fun of other people. It also involves manifested in several types of dangerous forms which involve no limited harassment, exclusions, impersonations, outing, trickery as well as flaming. Online bullies can also reach the targeted victims at several places. Moreover, it is necessary for distinguishing among the changing forms of cyberbullying, the complex terms of cyberbullying are presented below which involve outing, flaming, denigration, impersonation, trickery, exclusion as well as harassment.

a) **Denigration**- Denigration is related to the posting of fake information about the person or spreading gossip to damage the reputation of the victim.
b) **Exclusion**- The exclusion is the kind of Cyberbullying that the perpetrator excludes the individuals from the online group.
c) **Flaming**- The Fleming is a type of Cyberbullying that relates to the sending of vulgar, offensive as well as negative messages to the other person.
d) **Harassment**- It is the posting of vulgar and abusive words to get upset the victim (Xu, 2016).
e) **Impersonation**- It is the type of Cyberbullying which involves the perpetrator that pretends of becoming someone on the online platform that also interacts with other people and share the posts while pretending someone else.
f) **Outing**- The outing is related to the sharing the secrets of the victims, and the personal information of the victims to get them embarrassed.
g) **Trickery**- It is the process of convincing someone in revealing personal information and using that information to embarrass the victim.

1.2.3. Prevention of Cyberbullying

According to [3], Prevention from cyberbullying is very necessary it requires to be analyzed and monitored and comes to an end. There are several ways for solving the problem of cyberbullying. These ways can be implemented on an individual basis and based on authority which is listed below:

a) Always teach the kids not to share their personal information on online platforms such as posting personal videos and photos on a social media platform like Facebook and Instagram, it will get miss used by some other person.
b) Never share the passwords as well as the account details with any other person always keep this kind of information to yourself so that it should not get hacked by the other person who can misuse it.
c) The other thing is never to discuss personal matters on social networking websites, keep confidential information Limited among trustable friends and families and there is no need to share personal information with strangers on social networking websites.

1.2.4. Trojan related to Cyberbullying

In the words of [4], Trojan is completely related to cyberbullying as it provides opportunities for criminals to access the confidential information of the user for misuse in creating theft or data breaching. Cyberbullying always creates and leaves digital footprints, it develops useful records that should be used as evidence in support to stop the bullying. The combination of the trojan and cyberbullying is analysed based on the results of attacks that are related to trojan antivirus, corrupting the user software by using the trojan virus to create data theft for misuse. The malware also creates issues by destroying the processors' background system, deleting the important information of hardware as well as corrupting or contaminating the files of the system [5].
The **types of malware** are presented below: -

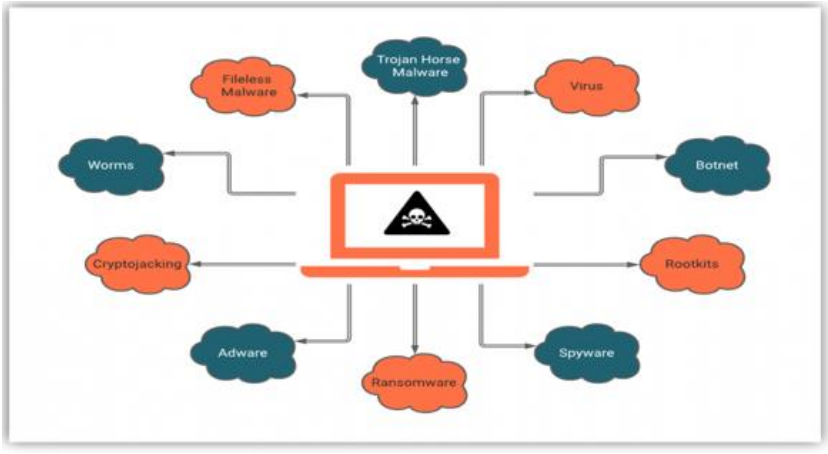

Figure 3 Types of Malware
(Source adapted from [16])

The image which is presented below represents the situation of the year 2016 of cyberbullying.

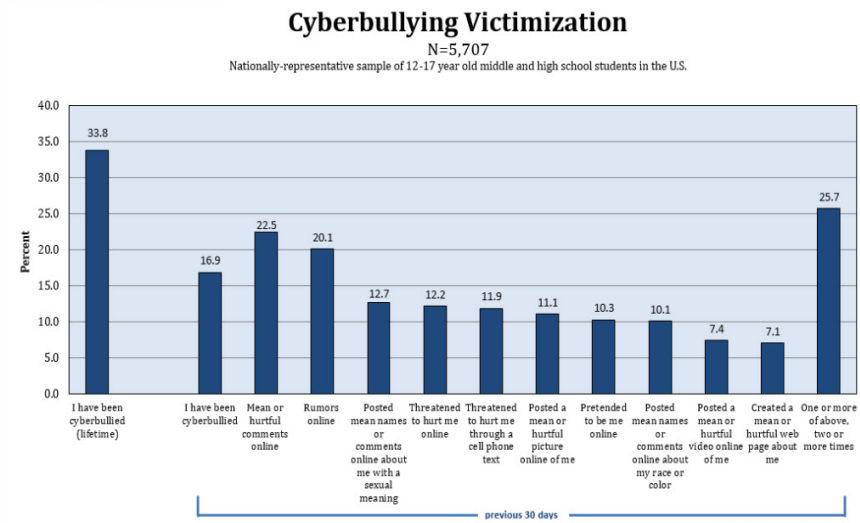

Figure-4 Impact of cyberbullying
(Source adapted from [24])

1.3. RESEARCH METHODOLOGY

The methodology which is used in this complete research is the qualitative methodology that is conducted on the basis of analysing the data of the previous years' records so as to get updated on behalf of the trojan antivirus which can create a very bad impact on humans and the system network. The complete methodology is followed through the descriptive methodology that includes the data analysis of the past times so that it can be compared with the results of the current times and the productivity as well as changes should be evaluated so that the necessary changes shall be created on the basis of the requirements of the current times [6]. This methodology is very easy and helpful in conducting as well as collecting the data on the basis of analysing the records of the past times. This methodology consumes less amount of time as compared to the quantitative methodology. The trojan-associated cyberbullying can be evaluated or analysed on the basis of the data of the past years. It can represent the exact situation and the improvements based on trojan malware and cyber bully.

1.3.1. Causes of trojan attack

The Malware can reach the computers through infected attachments, contaminated messages, or by the means of bogus web portals. Moreover, secret trojan services are also present which can be downloaded or installed on a system that is targeted remotely without getting informed by the user as well as without any kind of communication related to becoming a target. The trojan attacks take place when the security is less or the firewall does not work or maybe the email is not protected properly. In these situations, a cyber-attack can take place and confidential data can be leaked and it can be misused [7].

1.3.2. Prevention from virus

Some of the preventions that can help to protect the system from malware, virus, and other system bugs are listed below:

1. Use a good antivirus that is capable to protect your system.
2. You should have the knowledge to identify malicious programs.
3. Be wary of the attachments of the e-mail.
4. Always avoid downloads from a third party [8].
5. Use the firewall which is based on hardware as well as deploys DNS.
6. Always remember to do the autorun.
7. Always check the SSL at the time of dealing with e-commerce websites.
8. Back up the data on regular basis.

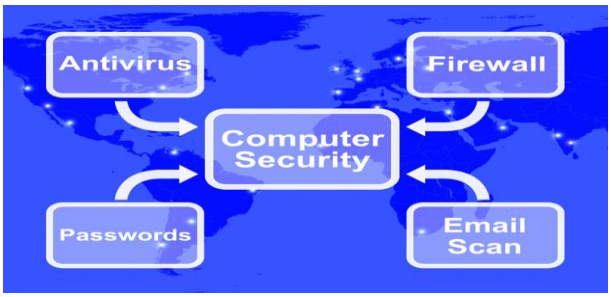

Figure 5. Prevention of virus
(Source adapted from [20])

1.3.3. Antivirus

The antivirus which can protect the system from the attack trojan are listed below: -

a) **Emsisoft Emergency Kit**- It is an anti-malware as well as an anti-virus tool for detecting and removing viruses, scanning, key loggers as well as other Malware threats.
b) **Malwarebytes**- It is this software that protects home devices as well as business points from Malware, malicious websites, Ransome ware as well as another kind of advanced threats [9].
c) **MalwareFo**- It is the Malware scanner that identifies as well as handles the files of ransomware at the time of testing.
d) **Spybot**- It is this spyware as well as the adware removal program of a computer that is compatible with Microsoft Windows.
e) **SUPER Anti Spyware**- It is the software application that helps in removal and detection of spyware, rogue security software's, Trojan horses, worms, and adware [10].

1.3.4. Blockchain

The block chain can be stated as an innovation that was created by fintech, it received a lot of attention since it gets originated as technology in enabling Bitcoins which are based on online transactions. Moreover, Bitcoin can be stated as a controversial form of currency that faces a lot of distrust and scepticism and it is also facing economic, social as well as legal impacts which are inadequately studied [11]. The technology of blockchain is acknowledged by the advantages of recording events and transactions. Several people believe that the blockchain is quite similar to the internet which revolutionizes how organizations and people like to manage transactions as well as assets. This technology of blockchain enforces the distributed consensus as well as the cryptographic transactions that render the uneasy situation of compromising within the integrity of records that may not get noticed in the network. Several experts believe on the fact that it is also capable of preventing malicious activities such as double sending as well as hacking. Moreover, many people are still present who believe that it remains sceptical [12].

1.3.5. Risks related to blockchain

The technology of blockchain is capable of preventing several kinds of malicious attacks as well as it also decreases several related risks but it does not neglect or eliminate all types of attacks [13]. The preventive mechanism can impair the opposition with other kinds of maliciousness as well as frauds, it involves the 51% attack, Identity theft on a digital basis, hacking, money laundering as well as takeover of an account. The table is presented in the image which represents the list of malicious attacks on the blockchain as well as the defensive measures.

Malicious Attack	Definition	Defensive & Preventive Measures
Double Spending	An individual makes more than one payment using one body of funds.	The complexity of the mining process
Record Hacking	Records in the ledger are modified or fraudulent transactions are inserted into the ledger.	Distributed consensus
51% Attack	A single miner node with more computational resources (51%) than the rest of the network nodes dominates the verification and approval of transactions.	Detection techniques; wide adoption of the blockchain technology
Identity Theft	The private key of an individual is stolen.	Identify and reputation blockchains
Illegal Activities	Parties transact illegal goods or commit money laundering.	Detection techniques; laws and regulations
System Hacking	The programming codes and systems that implement a blockchain are compromised.	Robust systems and advanced intrusion detection methods

Figure 6. List of malicious attacks on the blockchain as well as defensive measures.
(Source adapted from [22])

1.3.6. Prevention from attack using blockchain

The technology of blockchain comprises two specific kinds of activities which are record hacking and double-spending. The double spending activity takes place, if someone do a single payment more than twice while utilizing the single body of the funds, it is possible in the peer-to-peer system networking as the server or the propagation delays at the time of pending payments that are broadcast within the network which gets unconfirmed transaction on various Times [14].

The blockchain is capable to tackle such type of issues by providing minor nodes in solving the difficult mathematical problems concerning the verification of the transactions. The blockchain is also capable of preventing fraud which involves assets, currencies as well as credits. The best example of it is the tracking of all the transactions as well as registering the complete transaction so that it can be evidence of any kind of fraud that has happened. Moreover, the third-party absence also provides the opportunity of reducing the fraudulent, malicious, corruptive as well as illegal activities that get originated within the inside of the system [15].

1.4. CONCLUSION

It is concluded that Malware like Trojan was developed along with personal computers, the first Trojan is theorized in the year the 1980s and it was developed in the year 1990. It is the name of the virus on a computer that is having the property of camouflage among the forms of regular software which can be games, utilities as well as programs, or an anti-virus. Malware creates the issues like destroying the processor's background system, deleting the important information of hardware as well as corrupting or contaminating the files of the system. Cyberbullying can be stated as the umbrella of various kinds of bullying activities that are more severe than others. In this matter the terms go beyond mistreating, calling, or making fun of other people. It also involves manifested in several types of dangerous forms which involve no limited harassment, exclusions, impersonations, outing, trickery as well as flaming.

The Malware can reach the computers through infected attachments, contaminated messages, or by the means of bogus web portals. Antivirus can protect the system from the attack of trojans such as Emsisoft Emergency Kit and Malwarebytes. The blockchain is an innovation that was created by fintech, it received a lot of attention since it gets originated as technology in enabling Bitcoins which are based on online transactions. The technology of blockchain is acknowledged by the advantages of recording events and transactions. Several people believe that the blockchain is quite similar to the internet which revolutionizes how organization and people like to manage transactions as well as assets. The technology of blockchain comprises two specific kinds of activities which are record hacking and double-spending.

1.5. REFERENCES

1. "Cyber-crime effect on Jordanian society | request PDF." [Online]. Available: https://www.researchgate.net/publication/355730131_Cyber-Crime_Effect_on_Jordanian_Society. [Accessed: 22-Nov-2022].
2. "Cyber Crimes and Cyber Laws," National Law School of India University, 11-Mar-2022. [Online]. Available: https://www.nls.ac.in/course/cyber-crimes-and-cyber-laws-2020-21/. [Accessed: 22-Nov-2022].
3. K. -, By, -, A. Kori, and P. enter your name here, "Critical analysis of cyber laws in India," iPleaders, 02-Jun-2018. [Online]. Available: https://blog.ipleaders.in/cyber-laws-in-india/. [Accessed: 22-Nov-2022].
4. N. Jabeen and P. Agarwal, "Application of social big data in crime data mining: Semantic scholar," undefined, 01-Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/Application-of-Social-Big-Data-in-Crime-Data-Mining-Jabeen-Agarwal/c200abfe6f2cb9edc256a7fc22c4071b9a181675. [Accessed: 22-Nov-2022].
5. Bhandarkar AM;Pandey AK;Nayak R;Pujary K;Kumar A; "Impact of social media on the academic performance of Undergraduate Medical Students," Medical journal, Armed Forces India. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/33612930/. [Accessed: 22-Nov-2022].
6. "The development of digital society concept in Malaysia: An analysis of ..." [Online]. Available: https://www.researchgate.net/profile/Che-Hasniza-Che-Noh/publication/331221344_The_Development_of_Digital_Society_Concept_in_Malaysia_An_analysis_of_challenges_and_implications/links/5c6cc3894585156b570aa051/The-Development-of-Digital-Society-Concept-in-Malaysia-An-analysis-of-challenges-and-implications.pdf. [Accessed: 22-Nov-2022].
7. k Sudhakar and K. Poorna, "A study on usage pattern of internet, awareness about cyber crime among arts and Science College students in Coimbatore City," PSGCAS, 01-Jul-2019. [Online]. Available: http://ir.psgcas.ac.in/id/eprint/98/. [Accessed: 22-Nov-2022].
8. Y. S. Rao, D. Pradhan, T. C. Panda, and R. Rath, "[PDF] Digital Crime and its impact in present society: Semantic scholar," undefined, 01-Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/Digital-Crime-and-its-Impact-in-Present-Society-Rao-Pradhan/d1085600782afec4925f9fa3c306719d29d3a33c. [Accessed: 22-Nov-2022].
9. "Formal generalization of cyber bullying: A review study." [Online]. Available: https://www.researchgate.net/publication/351953711_Formal_generalization_of_cyber_bullying_A_review_study. [Accessed: 22-Nov-2022].
10. "A critical study of the violation of women's right in India with ..." [Online]. Available: https://bpasjournals.com/admin/upload/dynamic2/8IME-33-2019P148-155.pdf. [Accessed: 22-Nov-2022].
11. J. Shah, "Jigar Shah, a study of awareness about cyber laws for Indian youth," PhilArchive, 01-Jan-1970. [Online]. Available: https://philarchive.org/rec/SHAASO-25. [Accessed: 22-Nov-2022].
12. "Assessing law enforcement's cybercrime capacity and capability," FBI, 06-Apr-2022. [Online]. Available: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-. [Accessed: 22-Nov-2022].
13. "Download pdf | cybercrimes against women in India." [Online]. Available: https://www.researchgate.net/publication/344661625_Cybercrimes_against_Women_in_India. [Accessed: 22-Nov-2022].
14. "Supremo amicus volume 27 | December, 2021 ISSN 2456-9704 are Indian ..." [Online]. Available: https://supremoamicus.org/wp-content/uploads/2021/12/Yash-Singh.pdf. [Accessed: 22-Nov-2022].
15. D. V. B. H. U. V. A. N. E. S. W. A. R. I. P SUDHANDRADEVI, "A visual analytical dashboard on cyber journalism: An empirical review," Turkish Journal of Computer and Mathematics Education (TURCOMAT). [Online]. Available: https://turcomat.org/index.php/turkbilmat/article/view/12674. [Accessed: 22-Nov-2022].
16. "Cheap SSL certificates from trusted SSL Providers," Cheap SSL Certificates. Buy SSL/HTTPS Certificate $3.98. [Online]. Available: https://cheapsslsecurity.com/. [Accessed: 22-Nov-2022].
17. "What is application security: Types, Tools & Best Practices: Imperva," Learning Center, 12-Oct-2022. [Online]. Available: https://www.imperva.com/learn/application-security/application-security/. [Accessed: 22-Nov-2022].
18. B. Griffiths, "What is a trojan horse attack and how to prevent it?," Littlefish, 22-Jun-2022. [Online]. Available: https://www.littlefish.co.uk/insights/what-is-a-trojan-horse-attack-and-how-to-prevent-it/. [Accessed: 22-Nov-2022].
19. M. M. Ali, "Cyber crime: Determinants of preventing cyber crime: A survey resear...," Research leap, 24-Jul-2021. [Online]. Available: https://researchleap.com/determinants-preventing-cyber-crime-survey-research/. [Accessed: 22-Nov-2022].
20. F. Oduro, "How to protect yourself against computer viruses," SCG, 31-Mar-2019. [Online]. Available: https://www.scg.com.gh/2018/10/08/protect-yourself-against-computer-viruses/. [Accessed: 22-Nov-2022].
21. C. BasuMallick, "What is a trojan horse? meaning, examples, and prevention best practices for 2022," Trojan Horse Meaning, Examples, Prevention, 13-May-2022. [Online]. Available: https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/. [Accessed: 22-Nov-2022].
22. J. J. Xu, "Are blockchains immune to all malicious attacks? - financial innovation," SpringerOpen, 10-Dec-2016. [Online]. Available: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0046-5. [Accessed: 22-Nov-2022].
23. J. W. Patchin, "2016 cyberbullying data," Cyberbullying Research Center. [Online]. Available: https://cyberbullying.org/2016-cyberbullying-data. [Accessed: 22-Nov-2022].