PROPOSED ETHICAL HACKING FRAMEWORK FOR SECURE DELIVERY OF ONLINE EDUCATION

Vanshika Garg[1], Riya Ailawadi[2]
E-Mail Id: [1]83vanshikagarg@gmail.com, [2] riyaailawadi09@gmail.com
Department of Computer Science, Manav Rachna International Institute of Research and University, Surajkund, Delhi, India

Abstract-Cybercrime is a computer-oriented crime conducted over network. Ethical hacking is used to overcome this cybercrime situation, but it is still increasing day by day. This paper discusses the overview of cyber security, its challenges and ethical hacking. This also contains advantages and disadvantages of ethical hacking. Information has also been provided for different types of hacking.
Importance of cyber security has been highlighted for online education being provided these days in view of COVID-19. Case studies of zoom and teams Microsoft have also been discussed. Since none of these have been proved to be secured.
Framework has been proposed to make online education more secure and safe.
Keywords: Cyber Security, Ethical Hacking, Online Education.

1. INTRODUCTION

Ethical hacking and cyber security plays a very crucial role In the world of internet, as many a people depend on internet for exchanging of data or information through social media, e-mails as it is more easier , money transaction and e-banking and online shopping is very easy. There are many organizations and companies which have many sensitive and confidential data stored on cloud and they are afraid about it is security therefore cyber security and ethical having is very much important.

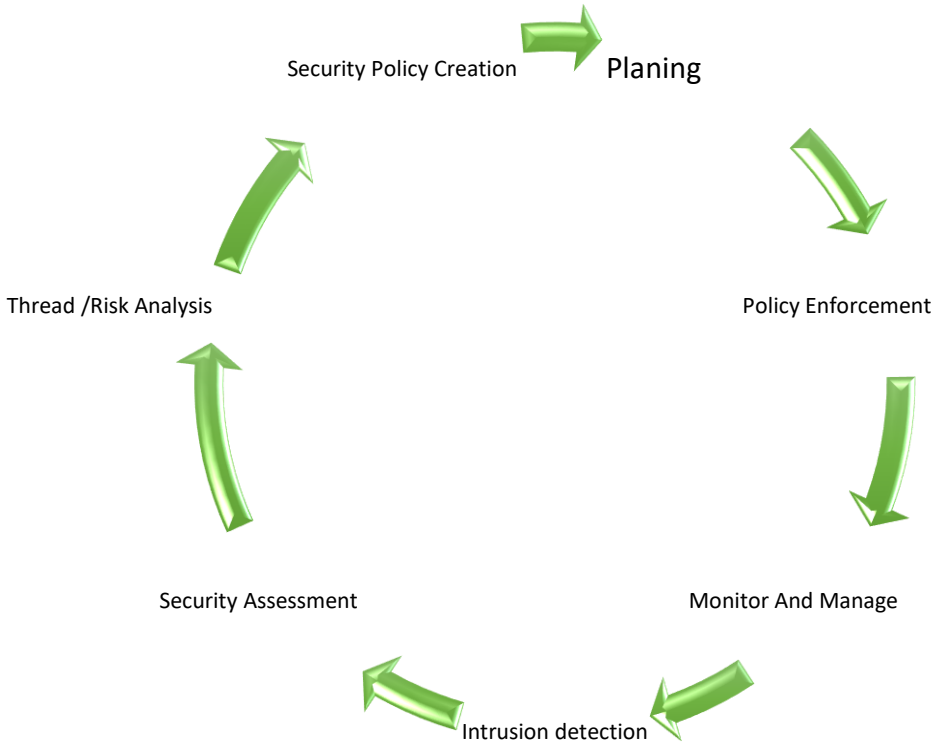

Fig. 1.1 Security Life Cycle [2]

1.1 Cyber Security

It refers to the security of various types of networks from attacks , it also referred to as information technology security . It protects the systems from unauthorized access or attacks and as well as from the disruption and misdirection of the services and data. As the need of computer systems and internet day by day so the cyber security plays an important role in today's world.

1.2 Cyber Security Challenges

1.2.1 Data Breaches

As many organizations have their data stored on cloud servers so, it will be an easy target for the attackers or the hackers to get a control over the data which is unauthorized and sensitive. [5]

1.2.2 Account Hijacking

As the information is stored in cloud storage, so it is easy for a hacker or attacker to keep a check on various activisties. Hacker can easily manipulate the Transactions and modify data that results to many frauds and software exploits.[5]

1.2.3 Exploited System Vulnerabilities

There is wide use of cloud computing these days. Many organizations share their databases and memory with each other which increase vulnerability. It also created a new platform for the attackers.[5]

1.2.4 Shared Technology, Shared Danger

On a cloud, we can share many applications and data if any type of vulnerability arise then it will affect all of the layers adversely.[5]

3 HACKING

It is a process by which a person who is a hacker or an attacker can modify the system features by using many techniques, tools and applications by gaining access for it. [6]

3.1 Unethical Hacking

It is being done illegally without taking any permission and is done with bad intentions. A hacker can insert virus or malware which can affect the data of the system. It is done to steal the data from the computer system or to do money transfer illegally. All this is considered as cyber crime. [1]

3.3 Ethical Hacking

It is also called as white-hat hacking. The ethical hacking is legal as in this process the person or the hacker takes permission from the organization. The hacker will check for the vulnerabilities existing in the system so that they can create a firewall to protect all the weak parts of the system. All this check is being done to make the information or data secure. As, many organizations find there data unsecure.[1]

3.3 Advantages of Ethical Hacking

- It provides the protection to services and marketing.
- It provide a better learning layout for business and talking about security. So, help in increasing the knowledge.
- Prevention against frauds and system exploits.
- Protection against malicious hackers.
- It helps in knowing about our own computer and network security system.[5]

3.4 Disadvantages of Ethical Hacking

- It can lead to data breach.
- It can be expensive as the hackers are specialized in their work.
- It can be very frustrating and time consuming for a hacker to secure a system if someone has hacked it.
- It can lead to the system failure and many errors could occur if not done properly.[5]

3.5 Classification of Hacker

There are seven kinds of hackers that fig. 3.1 shows:

3.5.1 White Hat Hackers

These are authorized and paid persons with good intentions who work for the betterment of the company, this hacker writes about its hacking and whatever work this hacker do is legal.[3]

3.5.2 Black Hat Hackers

They are also considered as malicious hackers. A hacker who do hacking just for his own benefit by identifying the weaknesses in the computer system and breaks into computer system without taking any permission.[3]

3.5.3 Grey Hat Hackers

These hackers have quality of both the black and white hat hackers. They may use some unethical methods but their intentions are not wrong.[3]

3.5.4 Script Kiddies

They are the most threatening people in terms of hackers. These hackers are an unskilled person who uses scripts or downloads tools available for hacking given by other hackers.[3]

3.5.5 Red Hat Hackers

They are also considered as the eagle-eyed hackers. Just like white hat hackers, red hat hackers also target to halt the black hat hackers.[3]

3.5.6 Green Hat Hackers

They are also non-professional in the world of hacking but they are bit divergent from script kiddies.

3.5.7 Blue Hat Hackers

They are much similar like the script kiddies; are beginners in the field of hacking. Blue Hat hackers payback to those who have challenged them or annoyed them.[3]

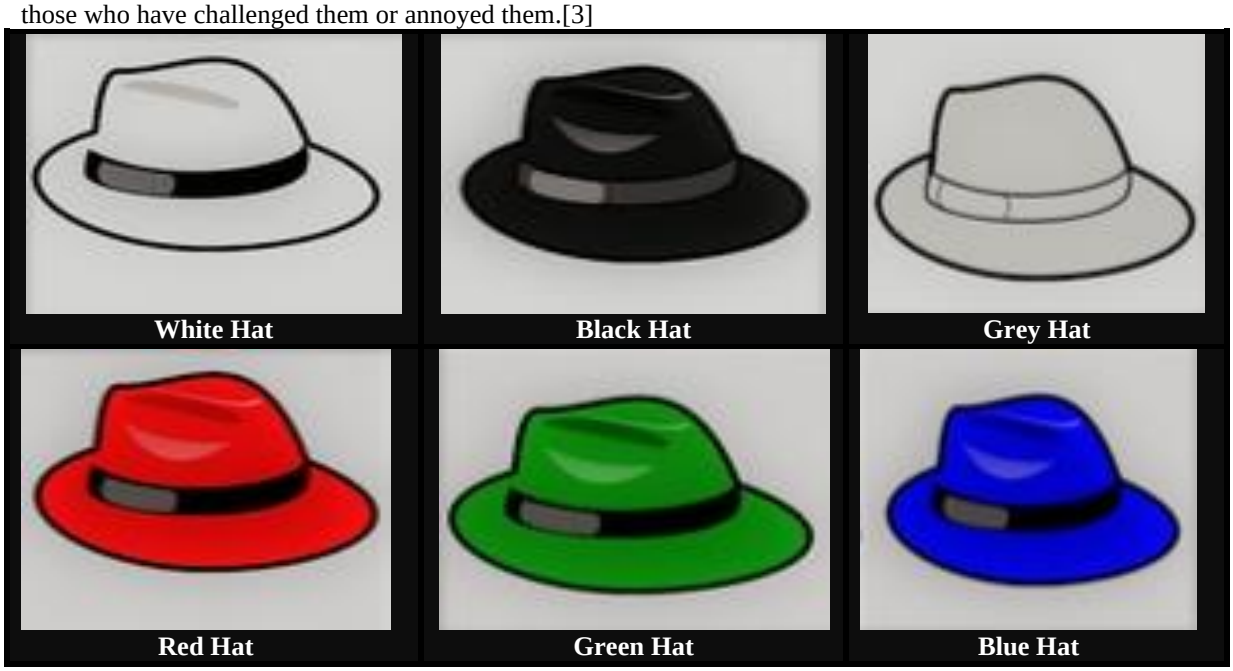

Fig. 3.1 Shows Different Types of Hackers.[5]

4. ETHICAL HACKING AND SECURITY AGAINST CYBER CRIME

4.1 Stages of Hacking

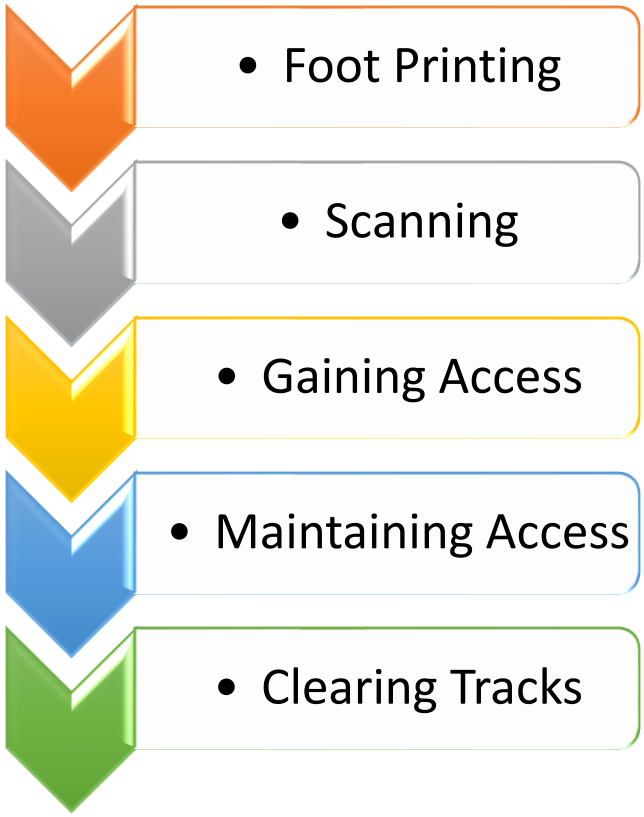

Fig. 4.1 Different Stages of Hacking [19]

4.2 Foot Printing

It is one of the preattack tasks that are performed before doing the actual attack on a computer system for gathering the information from it. It is a process of collecting information from the target system so as to penetrate into the system.

Foot printing helps to:

- Know the security configuration of the application and details about the firewall in the system,
- It will greatly reduce the number of attack area in the system.
- Loopholes and threads which are present in the system of an organization can be identified easily.[19]

4.3 Techniques Use for Footprinting

4.3.1 DNS Information (Domain Name System)

It converts human readable names into computer readable IP-addresses and vice versa.

4.3.2 WHOIS Query

It is used for querying the databases that stores IP address and domain name.

4.3.3 Network Enumeration

By this process, we can discover the number of devices on a network. The protocols such as ICMP and SNMP are used to gather the information.

4.3.4 Port Scan

It is a process of sending client request on a host and its main goal is to find an active port.

4.3.5 Scanning

It`s target is to identify the live hosts, ports and services. This process is used to identify the threats, vulnerabilities and loopholes in the computer network system.[19]

4.4 Techniques Use for Scanning

4.4.1 Ping Scan

It is used to check if the target is alive or not. If the reply is ICMP then the target.

4.4.2 UDP Scan

It is a process of sending packets to every targeted port. UDP scanning is generally slower and quite common.

4.4.3 Network Scan

It is used to find the topologies of the network.

4.4.4 Gaining Access

It is a process of finding holes which are present and if they are found then we enter through that hole and in this process we check for the vulnerabilities.[4]

4.5 Vulnerability Testing

4.5.1 SQL Injection

It is a technique which is used to insert the malicious SQL statements into an entry field.

4.5.2 Session Hijacking

It is also known as cookie hijacking. It is the done by stealing the session cookies and after stealing these cookies the adversary use the pass the cookie to perform session hijacking.

4.5.3 Directory Traversal

It is also called as DOT -DOT SLASH attack. The goal of this attack is to gain unauthorized access to the system.

4.5.4 Maintaining Access

When the hacker gained the access then he will not leave any evidence back. The hackers keep some backdoors for entering to the system when he needs to do so as he owns the system now.

4.5.5 Clearing Tracks

This is the final stage of the hacking. As all these processes have been done then at last this process is been performed to erase all the things that have been done in the previous phases.

4.5.6 On Different Functional Domains

Many of our important transactions, meetings and sharing of data happen over internet. While an increasingly connected world makes our lives easier, it also poses great risk as we expose our personal data to cyber criminals or hackers. The hackers have devised numerous ways to steal important data which is then put to misuse.

5. DIFFERENT DOMAINS

5.1 Business and Governments

As the account organization is been hacked then the hacker can do many money transactions due to this the company goes under loss. When the network or the system of any organization is been hacked then it results to a major loss of information because in many of the cases the important files or information is deleted or it could be changed. Sometimes the customer information is also been stolen and deleted. When the company is being hacked then they can pay for the initial damages but the main problem for them is there reputation as if any company, organization or a bank was hacked several times then customers lose their trust for them and they sift their accounts or orders to different banks or to different companies. As there reputation in the market gets bad then they lose their business. [5]

5.2 Health Care

Health care hackings are becoming more common it is quite concerning and reinforces the urgent need for health care organizations to continue maturing their cyber security programs. The hackers hack medical data of a patient as it contains patient's full name, address history, financial information, and social security numbers and all this information is enough for hackers to take a loan or set up a line of credit under patients names.

5.3 Banking

Bank's in order to enhance their customer base introduced many platforms through which their transactions can be done easily through internet but it increased frauds the main Frauds are credit card frauds and fishing. Doing online banking is not secured always due to increase of cybercrimes as many a website can take or save PIN card numbers, passwords, CVV numbers etc for misuse.

5.4 Stock Market

The data breaches have a long term impact on a companies stock price. Breaches that leaked highly sensitive information like credit card and social security numbers saw the larger drops in share price performance on average when compared to breaches where financial data was not included.

5.5 Prevention of Cyber Crime

We can prevent cyber crime by the following ways:

5.5.1 Use Strong Password

Keep distinct password and username mix up for each account and prevent the temptation to attacking methods like brute force attack, rainbow table etc.

5.5.2 Use Trusted Antivirus in Devices

Always try to use trustworthy and hugely progressive antivirus software in mobiles and personal computers. This gets to the prevention of distinct viruses attacks on devices.

5.5.3 Keep Social Media Private

Always keep your social media data private which are only visible to your friends only. And make assured only to make friend who are known to you.

5.5.4 Keep Your Device Software Updated

At any time you get the updates of the system software update the system at the same time because previous version can be easily attacked.

6. ONLINE EDUCATION

The increasing use of e-learning systems has been seen in past few years and the continuing growth of it been documented by numerous studies. With the increase of growth there is an increase in security issue in e-learning systems both in research and education. As the e-learning systems are open, distributed and interconnected so security becomes an important challenge in order to ensure that there would be no unauthorised access. [15]

Some of the benefits of using internet as education are:

- The biggest advantage is that it gives students as well as teachers the ability to access all different type of information.
- It eliminates dependence on conventional means of learning.
- It provides an environment suitable for collaborative learning.
- It removes the time and place constraints.

6.1 Cyber Security Threats in Higher Education

6.1.1 Viruses and Social Media

College and University students are the biggest users of social media which lead to spreading of malware and other viruses like wildfire through social media sites.

6.2 Consumerisation of IT

It has made situation more difficult to manage. As many users adopt their own devices for professional use, Higher education institutions will see more network security threats.

6.2.1 Cyber Security Issues for Distributed E-Learning Systems

- Systems are vulnerable to a range of security threats.
- Authentication: broken authentication and session management, insecure communication.
- Availability.
- Integrity attack: Buffers unflow, injection flaws, malicious file execution.
- Confidentiality attacks: Insecure cryptographic storage, information leakage and improper error handling.

6.2.2 Protection Measures

- Installing firewalls and anti-virus software.
- Training security professionals.

- Implementing security management.
- Using digital right management and cryptography.

7. APPLICATIONS

Zoom app is super easy to use and convenient it is been used by the business sector as well as by many education institutions fig4 shows. Zoom app contains many features such as video conferencing, cloud conferencing, file sharing, wireless content sharing, virtual meetings and integrated audio features into one easy-to-use platform.

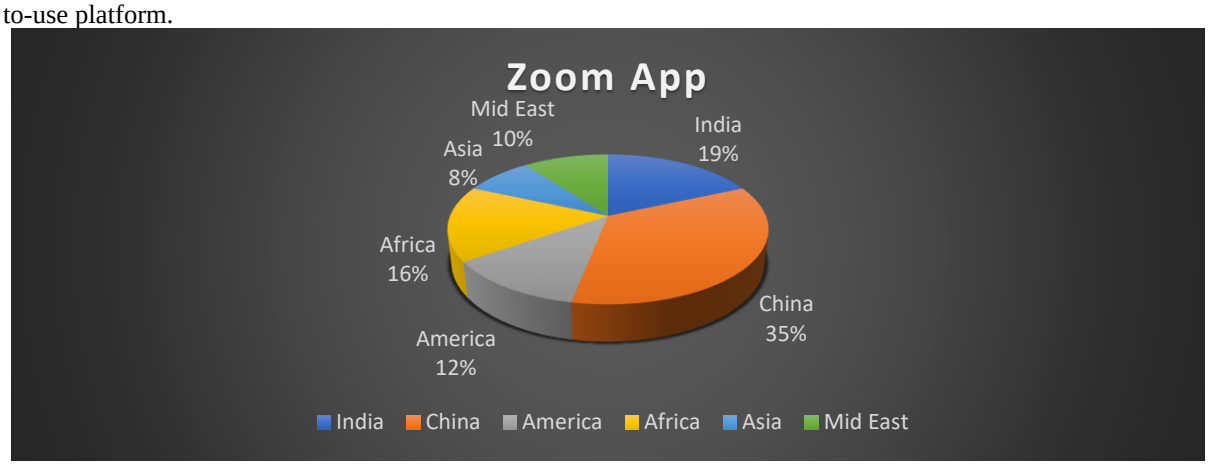

Fig. 7.1 The Percentage of Users for Zoom App from Different Countries

7.1. Educational Sector

This platform is very much useful for many educational institutions as online classes are been conducted and the information is being shared to students easily. So that there will be no academic loss.

- Students and teachers can record these classes so that they can see them again.
- Students can easily interact with their faculties and ask about their doubts. It has some disadvantages also like.
- This platform is not fully secured as anyone can enter to the classes without any permission of the organizer as any sever can easily hack their passwords and room codes.
- Students can also face many problem related to their assignment as when they share them with their faculties then any student can get their assignments easily.
- Many higher authorities could face many problems while interacting with faculties and sharing important information as there could be Data loss as the person who is sending data is not sure that information which is been send is only shared to that person or someone else could also access it.

7.2. Business Sector

This app is a good platform for business purposes as they can connect with their clients and employee.

- By using zoom rooms they can stream dual screen for different employees at the same time.
- It works for almost every operating system PC, Mac, Linux, iOS, and android so employees are not locked into specific devices.
- There are many security issues related to this app like.
- Zoombombing, which let's anyone easily hack into the meetings and show inappropriate content which is not good for the companies as they have many confidential details and if anyone tries to enter their meeting then it would let to business loss.
- The meetings are not end-to-end encrypted, zoom data is decrypted at the server which means the company can see and hear the conversations which is not good.
- There was the problem with Zoom's installer, which took over admin privileges to gain access to a user's computer. That access could be misused to install programs without the user's knowledge and to gain access over the documents of that system.
- Zoom collects Data from the system and was found to be sending data to Facebook, even if you were not logged in to a Facebook account. Due to all these problems, many companies decided not to use this app for online communication as it can lead to data loss.

8. TECHNIQUES

The methods by which we can secure our system while using this app are:

8.1 IPS (Intrusion Prevention System)/IDS (Intrusion Detection System)

It is a network security and threat prevention tool. Used to examine network traffic flows in order to find malicious software, record detected threats, report detected threats and take preventative action to stop a threat from doing damage. An intrusion prevention system will work by scanning through all network traffic. Therefore, it is a useful tool to examine if any malicious software is installed in the system. [13]

Both IPS and IDS tools will read network packets. IDS tells about what actions are taken next but will not take any action on its own. An IDS requires a human to analyze results and make decisions on what to do next. This

is why IPS is seen as an extension to IDS. For a small-scale purposes these both are been used to detect, report and prevent the threats and any malicious activity. [13]

8.2 TLS (Transport Layer Security)

It is based in TCP/IP protocols it takes advantage of both symmetric encryption and public key encryption for securely sending private data. It has features like authentication and message tampering detection. By using this data encryption is been provided so that there will be no data loss. Every time there is digital certificate verification, which has it is expiry also. In this process as long as the server can successfully decrypt the client's message with the shared key, it sends along a confirmation and its own "Finished" message with encrypted contents. This method is been used for the large-scale purposes. For big companies and industries, this method is very much useful to secure their data. [13]

8.3 Another Application

On the other hand, Microsoft Teams is a much safer app as compared to zoom app. This app is been used by many educational institutions and schools to connect with their students and staff members. It is a very convenient way to communicate online as well as it is very much safe.
On this app, the sessions can be recorded and anyone can watch them later on if they missed that session or want to go through them again.
It is very much safe for students to upload their assignments as no one can see their assignments expect their faculty who assigned it to them. Therefore, that no one can steal their assignments and just copy them.
It is very easy to conduct online examination on Microsoft teams as teachers can examine students easily by making their cameras on during examination.
Therefore, overall it is a very easy and safer platform to communicate.

9. FUTURE WORK AND CONCLUSION

In this paper, we have discussed the key terminologies related to Cyber Security. Importance of Ethical Hacking has been highlighted along with the ways the cyber crime is conducted in different domains of our day-to-day life ranging from online financial transactions to online repositories existing for patients to online delivery of education. In short, these days, each and every one is vulnerable to cyber crime because of the way, online data accessibility is increasing. In this paper, we have also discussed two case studies for online education portals being utilized amidst COVID-19. Two security techniques have also been discussed to ensure secure delivery of data from one place to another. However, a complete framework still needs to be worked upon for ensuring the secure delivery of data. Hence keeping in mind the current perspective of online processing of data and its security relevance, we are going to propose a framework that will ensure the secure delivery of online education where details will not be trapped in between by untrusted parties during the transmission.

REFERENCES

[1] Neeraj Rathor “Ethical hacking & security against cyber crime”2015.
[2] K. Bala Chowdappa, S. Subba Lakshmi, P.N.V.S. Pavan Kumar “Ethical Hacking Techniques with Penetration Testing”2014.
[3] P. Harika Reddy Surapaneni Gopi Siva Sai Teja”Cyber security and ethical hacking”2018.
[4] Deepak kumar[1], Ankit Agarwal[2], Abhishek Bhardwaj “Ethical hacking” 2015.
[5] Deepansh Kumar, Yugansh Khera, Sujay, Nidhi Garg, Prateek Jain”Towards the impact of hacking on cyber security”2014.
[6] Susidharthaka Satapathy, Dr. Rasmi Ranjan Patra “Ethical hacking”2015.
[7] Asthana, N.C., and Priyamvada Asthana. ”Cyber Security, Cyber Attacks and Hacking”2013.
[8] Hall, Gary, and Erin Watson “Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security. Create Space Independent Publishing Platform” 2016.
[9] Moore, Robert “Cybercrime: Investigating High-Technology” 2006.
[10] Michal Korcack and Jaroslav Lamer and Frantisek Jakab” Intrusion Prevention/Intrusion Detection System (IPS/IDS)”.
[11] Sunit Belapure Nina Godbole “Cyber Security: Understanding Cyber Crimes”2014.
[12] Noluxolo Kortjan “A Cyber Security Awareness and Education Framework for South Africa”.
[13] Luis corrons “A Look back on Cyber Security “2012.
[14] G.Nikhita Reddy, G.J.Ugander Reddy “Study of Cloud Computing in HealthCare Industry” 2013.
[15] Avanthi Kumar “Safety Critical Systems Cyber security”2014.
[16] K.Bala Chowdappa, S.Subba Lakshmi and P.N.V.S Pavan Kumar “Ethical hacking techniques with penetration testing”2015.