***Cyber Physical System – Advances and Applications, 2022, 1-31***

**CHAPTER 1**

**An Analytical Approach to Rescue Automation from External Assaults**

**Isha Singh1 and Jagdeep Kaur2 \***

*1Deptt. Of Computer Science and Engineering (Hons.) Information Security, Chandigarh University, Punjab*

*2Deptt. Of Physics, Chandigarh University, Punjab.*

[Jagdeep.uis@cumail.in](mailto:Jagdeep.uis@cumail.in)

**Abstract:** There are many Machine Learning and AI based attacks which can destruct the data as well as the systems too which are IOT based and the things connected to internet. We are going to discuss the same data with the help of developing the in-built software within the product to stop all the offences.

The research is being made on the basis of positive as well as negative sides. Most of the times, no such action is taken in regard to protect the system when offence takes place as no option is there in response to it.

So, in order to rescue we will be trying to develop a ML based software with C++/ C/ Python to stop the action of these sort of attacks. Safety from Viruses, Threats, and offences will be done with the help of the antiviruses and by applying the layers of firewalls.

This in-built software will automatically detach the USB Killer or consume whole battery of it so that it won’t work when it will find that it is not appropriate for the system as soon as it enters the system and will stop the destruction of the system. And our try will be that also that USB rubber ducky also that can hack the data with few codes added in that already. So, for that we will try to build a code-based AI system that can stop the hacking of the system and leading the person to stay calm.

**Keywords:** AI Based, Cyber Laws and ethics, CIA Triad, Data Breaches, Data Mining, External Assaults, Frauds, Human Interface Device (HID), Hacking, Internet of Things, In-built Software, Machine Learning, Programming Languages, Security, Threat modelling, USB Killer, USB Rubber Ducky.

**INTRODUCTION:**

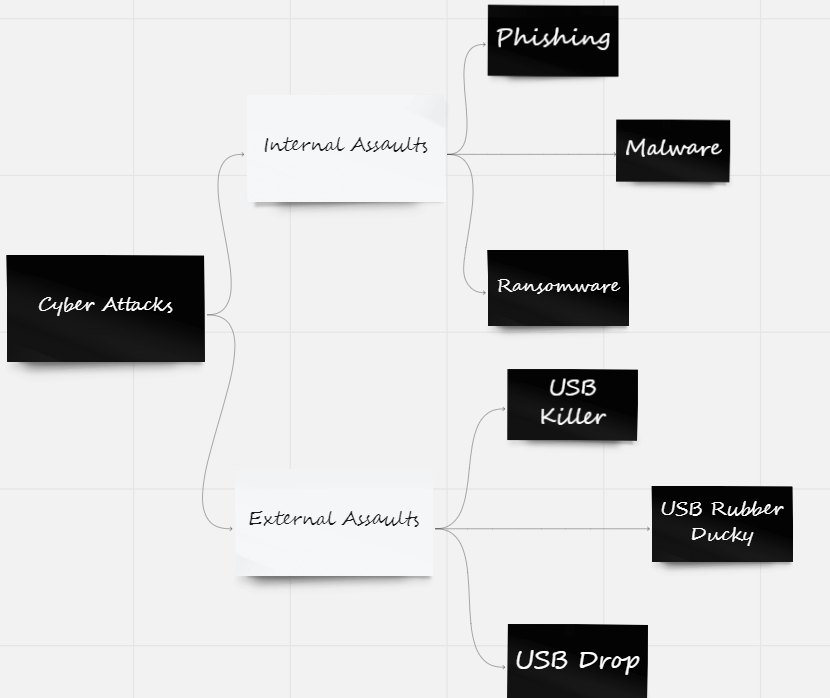
What Cyber Security means all over the world? This is what we are going to read and discuss in this particular chapter. And also, this chapter will describe all the threats which comes under.

As soon as the Internet came into existence human life became easier as well as the dangerous too. In the way the internet helps us it also is hazardous as it welcomes few problems without any information to the user. This is the reason that Cyber Security took birth in the field of technology i.e., information technology (IT) security. And, these attacks (internal and external) for which the Cyber Security came.

**Cyber Security**

Cyber Security is basically a technology which is a sort of shield to the network, information, data, hardware, software and from any type of disruption to the necessary things related to technology. It helps to decrease the problems faced due to cyber-attacks, crimes and frauds. The important task of the Cyber Security is to safe guard the IOT. There are many internal and external attacks happening all around the world with no knowledge to the user whether it is individual or an organization. These attacks prohibit the user to work safely and securely. Cyber Security covers the most important required objective i.e., CIA triad (Confidential, Integrity and Availability). This CIA triad is what shows how Cyber Security works and what are its priority. It only carries the aim to preserve the user’s data and information.

And, Some of the Cyber Attacks are mentioned below with their types and our shown in pictorial form on the next page:

**Cyber Attacks**

**Figure 1:** Types of Cyber Attacks and Diversions.

In this context, it describes that, there are cyber-attacks which are further divided into two types: “Internal and External Assaults”. These assaults are expanded and are of many types which damages the system in different ways.

1. **Internal Assaults of System**

Internal Assaults are those which take place in the presence of the Internet. These assaults basically damage the software and increases the risk to steal the most sensitive information of the user which can be related to business, personal such as passwords of bank accounts, can destroy credit cards, make purchase and many more. These things can sometimes happen without any information to human beings. These attacks are mentioned as Internal Assaults since they occur internally i.e., just in the system and no external thing or device is used to make these assaults happen. Even these cyber-attacks can be easily executed from remote areas on someone’s system so as to Hack into their privacy.

**Types of Internal Assaults**

There are many types of Internal Assaults such as Phishing, Malware, Ransomware, DDOS, SQL injection, Man-in-the-middle attacks, etc. In this context, only few of the attacks will be discussed below:

1. **Phishing:** In this attack, the user is attacked by the hacker by sending uneven trickery messages or mails in order to steal important information so as to get into the privacy of a common people. One such example of it is Spamming. It spams by sending useless mails which acts as useful to obtain the confidential reports or personal information and demands ransom from them which is called as Ransomware.
2. **Malware:** As demonstrated, a software is deliberately developed as a link and mixed in between with the original one and the common people will not be able to differentiate between the fake and the real due to what they will click on the fake link leading to the huge threat of leaking their own personal information and also leading the attacker to gain unauthorized access to system.
3. **SQL Injection:** An automation to enter the codes which are filled with SQL statements to destroy the data of the system with those malicious codes which are meant to damage or rob the private database.

There are few more different types of Internal Assaults which are used by the hackers to attack your system and leads to increase of the rate of Cyber Crimes.

1. **External Assaults of System**

External Assaults are the assaults which are said to work in the absence of the Internet. These assaults generally damage or attacks your hardware as well as the hardware. These are caused by injecting external devices. These attacks are known to be the external assaults because they occur when any external malicious source is injected and they are pirated with either lots of viruses or they carry such codes which are unhealthy for the system. For these crimes, external devices are required to rob.

This type of attacks or assaults enter in the computer due to the pirated CD, DVD, USB Drives. In the pc, USB ports acts as a connecter. And, now a days there are many USB thumb drive similar to simple and original pen drives but actually are not the simple USB drives, they are more treacherous and are operated by hackers to exploit or extort and play with the data. And, for many of these there is no action in response which are still used to theft the data from computer or the IOT based things quickly and it is all because of these external assaults or USB attacks are HID due to what they are unable to detect.

Before getting below to the types of external USB Attacks, we have lot to discuss about USB.

**What is USB?**

USB stands for **U**niversal **S**erial **B**us**.** This is a sort of technology said to be a way of communication with the system through output device. This is externally inserted and is connected through the USB ports of the system. By these USB ports, we can also connect the wireless mouse or keyboard by inserting the small USB like small device. This have developed many forms to get connected to the system or mobile. They are also power supply which shows that these are also present in the mobile phones and are inserted through the peripheral device. Those are power cables which not only charges the device but also transfer data from one device to another. Similar is the situation in the devices like laptops, computers or system i.e., the USB ports are present in here also through which we can transfer data in either the pen drive or the system. This USB was introduced to General Public License (GPL) in the mid of the 1990s something and USB Thumb Drive came in the world here by the start of the 2000s according to the article read on Google. This shows that USB Thumb Drive came soon after the USB is instigated.

This is not always possible that one USB Drive which you are using is always and every time safe and protected. These output devices can be sometimes very threatening to use as it causes a big trouble to the system of either a common person or an organization. Some of these devices are now considered as external USB attacks which are well said as Human Interface Device (HID).

The list of HID i.e., the USB external attack is a medieval history of Cyber World since 2010. These attacks frame the system quicker than the online internal attacks that a user can’t think of. This is how all external assaults work and there are many of them. So, types of external assaults are mentioned:

**Types of External Assaults**

Many of the USB cyber-attack are counted under the external assaults such as USB killer, USB Rubber Ducky, USB Drop Attack, USBdriveby, Evilduino, Default Gateway Override, Virtual Machine Breakout, etc. There are some 28 or 29 external assaults (USB Attacks).

Here, only few of the attacks are discussed below:

1. **USB Killer:** This is very similar to a simple USB thumb drive which do not look harmful at all to the system but is actually very dangerous to the pc. As soon as it enters the USB port of any system it kills that and permanently destructs the device badly as it sets an electric surcharge and destroy that system in just few seconds. This can be a huge loss to the user. And also, to this assault there is no safety which can safeguard the object to protect from this assault.
2. **USB Rubber Ducky:** This is a perfect hacking technique which is also similar to the pen drive and it consists of already inserted keystrokes. When this is entered in your device, this will work as a keyboard and which leads it to take hold of your pc and your device will lead the already inserted keystrokes to work and that will hack your system. And, it types so many words in a minute that the user will be confused and till the user won’t be able to work due to constant typing of unnecessary set of codes.
3. **USB Drop Attack:** This attack is performed deliberately by the attacker/ hacker. In this attack, a normal looking pen drive is kept strategically by the attacker which is filled with lots of malicious codes and which is when plugged into computer hacks into the system to steal your sensitive or private information or damage the data.
4. **In Smartphones via USB Ports:** This attack takes place is mobile phones through there USB ports. This attack, creates obstacle in smartphones as the hacker uses mobile charger as a domain to store and transfer malware to the smartphone to hack the smartphone without letting user to know about it.

There are many more external USB assaults which are hard to understand and as discussed above these attacks are complicated to detect because they are all HID. So, in this chapter we are going to propose an idea for two of these assaults which might help to resolve the problem and make IT (Information Technology) easy.

**Review**

Lots of research and reviews are made which reveals the interesting facts, in-depth knowledge and historic events happened in the past as well as are still being done. This conveys that research is a brief of what achievements or studies were done to communicate knowledge between the past generation and the present. From this, the representation of the importance of Cyber Security is known. According to the study, NCRB (National Crime Record Bureau) cybercrimes in the cyber world had increased in the past few years that automatically grows the threats, offences and attacks leading to a doubt on the IT world. Few of the topics which are targeted mostly are mentioned below:

1. **Internet Security:** This is also known by many names such as cyber security, network security, technology security, information security, IT security, and many more. This cyber security came to the reality when this cyberworld was created soon after that as the threats, offences had taken birth very fast just after the Internet is made available in some 1970s which was created by BOB THOMAS to secure the IOTs and networks from extortion. Here in, threat modelling narrates threat attacks and the federal learning to those attacks leading for solution to defend the data and system as well. National Security/ Government Security, is as required as the private organizational security. The most popular government organizations like DRDO (Defence Research and Development Organization) and many others help to keep the protection shield to prevent major details of our country. Once in the study, was told that India’s Cyber Security was a big failure at the times of PRISM program but just after few amendments India became the “Authorizing nation” for the IT product. “Social Engineering” states the data of the attacks, attackers and strategy for the attacks.

The History of USB thumb drive is started since their presence seems in reality by 2000s and the list of the USB based attacks get to recognized since 2010 and the USB killer and USB Rubber Ducky (Bad USB’s) came to industry where they were seen to be so popular.

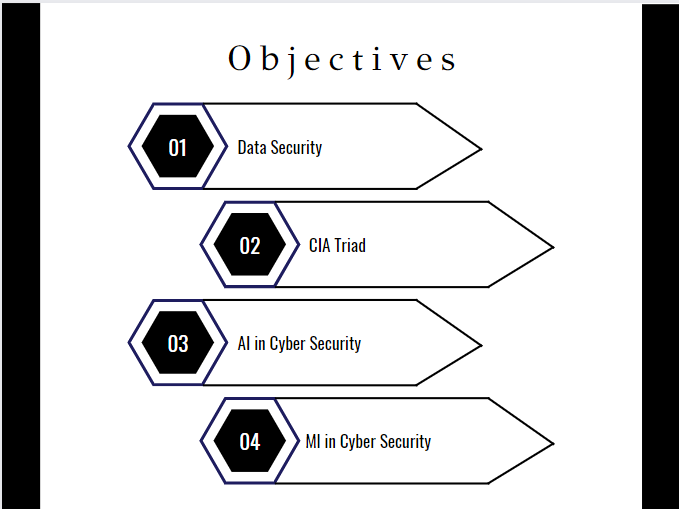
1. **USB Killer:** It is also known as the “Kill Switch”. This was made for the testing purpose. This is developed by DARK PURPLE in 2015. It is HID which restricts it from getting detected. According to study, it was designed via GitHub in Python programming language. Old version of USB Killer, it doesn’t have internal battery. It charges from the USB port of the system it is connected and discharges the data due to power and electric discharge. Risky at that cost, it is dangerous for both the physical and hardware security. In the 2019, it was found with the college student of St. Rose in Albany of New York who intentionally installed this and destroyed some nearby 57 computers of the college. As for the new and recent version of USB Killer stated to be the offline maintained attack as it doesn’t required power because it have internal battery. It is told that it can be used unlimited times. It is said to be an electrical attack/ assault. It is the USB based attack which can damage the hard disk.
2. **USB Rubber Ducky:** It is well known for being the same hacking attack or technique as the USB Killer as they both pretends to be a normal USB Thumb Drive or pen drive and acts as a HID. This device was just pretended to be said as the tool for the penetration testing but actually a suicide for the device which cannot be detected even. It was made in 2010 and it consists a set of preloaded malicious codes which is when injected into the system through USB port covers the whole screen of the system with the codes without even providing user a second to think about the process that is happening in front of the user. USB Rubber Ducky uses few of the commands which are pre-set in the

drive. These commands give a temporary pause in the program giving operating system (O/S) sufficient time to execute the code and program so that another command can process the next word present in the script of ducky. It doesn’t allow user to interact with his/her own system and the person unknown to these assaults will sacrifice their data to the attacker easily and will suffer. Thus, these attacks aware the common people to avoid the usage of unknown devices. They can be pirated or filled with unsuitable malicious codes.

**Comparison**

There are many techniques which are described to safeguard the system for the security purpose. Artificial Intelligence (AI) and Machine Learning (ML) are the technologies which help in solving few of the problems related to the attacks and assaults. There are some of the main purposes of the Internet Security which are necessary to know. The cyber laws and ethics are also needed to be look after just to avoid the violence of the rules in the cyber world.

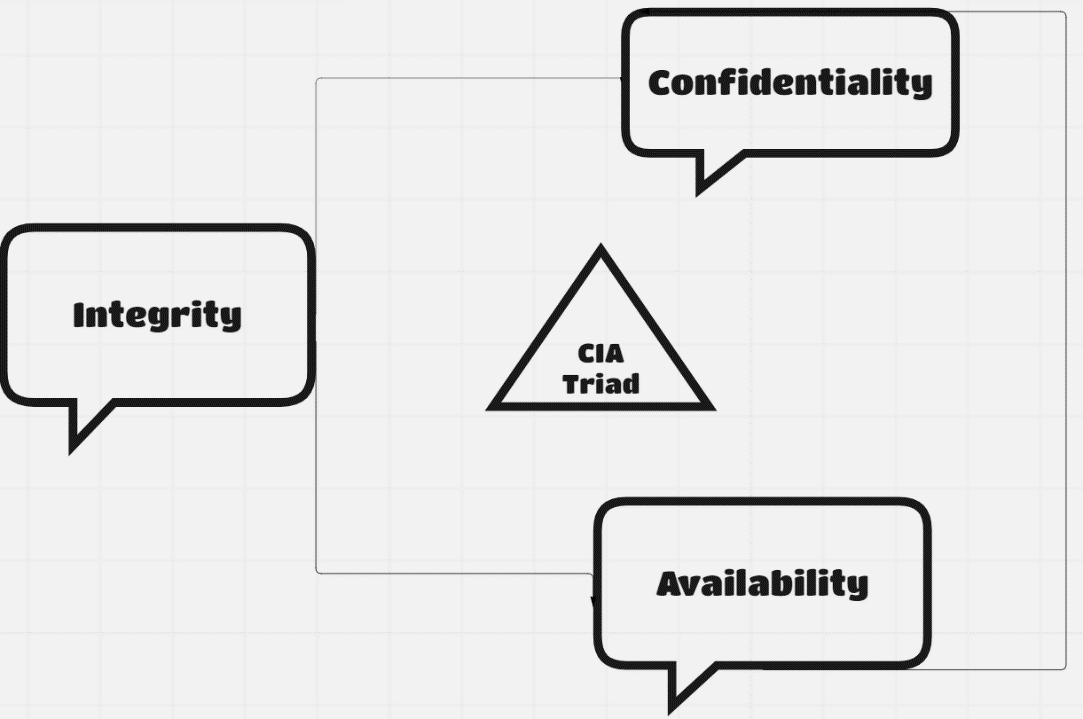
According to the study, the objectives we came across during the whole evaluation for this are:

****

**Figure 2:** Main Objectives

1. **Data security,** Internet is full of vast network connections and those connections contains lots of websites which are made of many webpages through which whole day long we all keep surfing without any knowledge whether these sites or webpages are safe to use or not. Some of the websites or webpages are developed deliberately by the hackers or attackers. They intentionally leave the links of these websites/pages which looks amazing to surf around and are very attractive that makes you to login or signing in to that site and this is how data breaching takes place. And, the users became the target of the illegal assaults and frauds. Data security is a big necessity in this field as once your data is robbed by the Hackers than it welcomes many of the threats, attacks and assaults. So, Data Security is very important.
2. **CIA Triad,** this is the main and the very important objective of the Cyber Security which is considered to be the very requirement of each and every person in this world. The entire group of customers wants the prevention and protection of their systems as well as the data. “This CIA stands for Confidentiality, Integrity and Availability”. This helps in prevention of the access, modification and ensure timely and reliable things to get information. Confidentiality helps the prevention from revelation of data by unknown or someone unauthorized. Integrity refers to the protection of system from the changes of the data by unknown user. And, The Availability provides the anticipation towards the access of the system i.e., who is authorized user to access the data and system. These three complete the triangle of the CIA Triad. For the safety of the system, this objective should be there to safeguard IT.

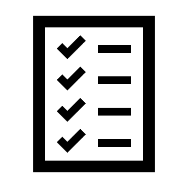
CIA Triad shows the three main components of the IT security. It properly shows how the security works and how it safeguards the system and data of the user as well as the organizations. Its diagram on the next page shows the proper full forms of each and every word. This is what CIA triad is. Mentioned below:



**Figure 3:** CIA Triad (Confidentiality, Integrity and Availability)

1. **AI in Cyber Security,** AI stands for Artificial Intelligence. There are lots of benefits of having this technique all over the world in today’s generation. This had made the work of the human beings reliable and smooth. Similarly, this works same in the field of Cyber Security. It is a vast technique which have many scopes and it also helps to develop wonderful techniques. We have observed lots of AI based tech which are an inspiration to more of the upcoming to develop the tech in order to have a more secure future. AI in Cyber Security, is a well source. AI can manage to quickly observe the different threats happening and also, the risky nature of the system that suddenly appears. AI security manufactures a strong base to identify the assaults and attempts to solve crises based on lately observed activities. There are few examples of the AI security such as: In surveillance like CCTV, Threat screening for large events, underside vehicle bomb detection and etc.
2. **ML in Cyber Security,** ML stands for Machine learning. It is a subset technique of AI. ML is a technology which helps to build a

software by preparing the well-organized algorithm. ML in Cyber Security differentiates between viruses and threats to defend from them. This can even set up software and machines to quickly observe and recognize the malicious codes and abnormal behaviour of the malware or attack present in the system. ML assists the data analysis too with this we can manage data of all types of activities or assaults or attacks due to which it become smooth and helps detect those frauds and stop the evil activity of the Hacker.

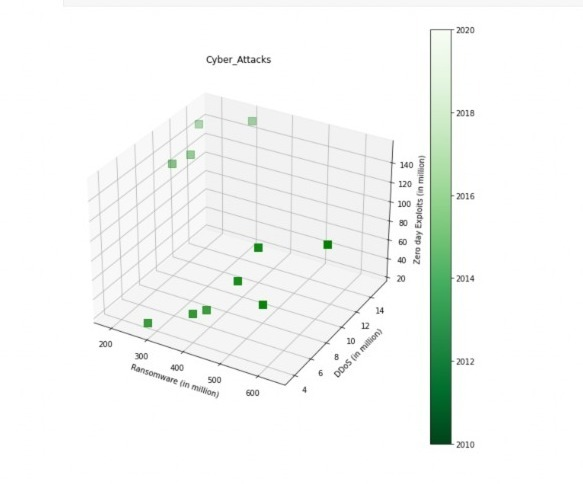
****

**Note:**

Cyber Security and Information Security are not same. They sound quite similar just because they both acquire the purpose of the security. They both have different meanings and definitions but yes, they are same in the terms of Security only. Cyber Security protects information from many sorts of attacks, threats in cyber world and handles the cybercrimes, cyber frauds and online attacks. It prevents the information from the cyber terrorism also whereas, Information Security safeguards the data in the cyberworld from all kind of attacks. This blocks the abnormal behaviour and unauthorized access. This did not let any unknown user to access and transfer of the data.

**Cyber Attacks rate from 2010 to 2020**(Data of Different viruses):

This is prepared with the stored data of the attacks happened in years of 2010 by using Python programming language in 3D- form which shows a 3D heat map graph of the cyber-attacks like Ransomware, DDOS (Distributed Denial-of Services) and Zero-day Exploitations and a grid mentioned with years from 2010 to 2020. In this, pandas’ function of the python is used for the data set and there are 3 columns which are for plotting and 1 column for the colour bar. To add 3-D data set sub-plot function with projection “3-D”. And, the graph is shown in the form of scatter plot.

**

**Figure 4:** Rate of Cyber Attacks from 2010 to 2020.

This figure shows the increasing rate of the risk due to Cyber Attacks. Don’t you think that Risks should be managed or Risks management is necessary in this field? If yes, then what type of risks are there which should be taken care and what types of risks are there?

Risk Management is not completed on its own. It needs guidance and have lot of people behind this to govern, maintain and secure data properly.

**Risk Governance:**

A well-known Cyber Risk Governance is a very crucial state where board of directs are authorized to guarantee that all the IT security is perfect to protect from the Cyber Threats and training the full section by entirely making them all aware about the security governing the commands for the better purpose.

This is Risk Governance which is required for managing the risks in the Cyber World. Now, what are the risk categories for what this Risk Governance is a big necessity. Risk Categories are:

**Risk Categories:**

1. **Strategic Risk:** This states the unnoticeable activities which badly affects the organization’s main objective and this is where the “Risk Governance” plays role in prioritizing the major acts for defending the site or system from assaults.
2. **Reputational Risk:**  This risk states that vulnerable activities related to Confidential, Integrity and Availability (CIA) Triad of customers, clients or community. This is where the management to safeguard from risks takes place and becomes the necessity.
3. **Financial Risk:** It states to the increase in the risk related or connected to capital or finance either they are short or long. This is now a days the most precious to the common person as well as the whole organization handling large accounts of finance.
4. **Compliance Risk:**  This risk is something which is relatable to danger to policies, laws, ethics and regulatory requirements. Policies, laws and ethics are very much important to someone as if they are disturbed than it is hitting on the principles of people as well as the community very strict to the laws. It can be considered as a type of national security as well or Social Cyber Security.

This is how Risk management is important in Cyber World and which should be done keeping Cyber laws and Ethics in mind always. It is a crucial task as the attacks are dominating from last few years. This is not always possible to have some solution to many situations but thinking out of the box and a clever thinking in a different makes us unique from the crowd. Proposed work shows the solution to the increasing risks with an appropriate management. So, the work proposed for few of the external USB assaults, a huge risk in the Cyber World. Inspiring everyday to protect the world form unkind malicious activities.

**Proposed Work**

The two devastating USB assaults/attacks commencing deadly loss to the system being the HID, yet is complicated to detect. Due to this detection problem, there is no solution to resolve these problems till now for those two USB attacks. These devices are built as penetration testing tools for the system but these turns out to be the attacking device which now a days is well known for the best hacking external technique. For every problem there is a solution. Similarly, for each of the assault we researched and came up with the solution and hope to be the good solution for these two attacks. So, we detected different “In-built methods” to safeguard data as well system.

So, the proposed work of the USB Rubber Ducky and USB killer are mentioned one by one below with their problem statement:

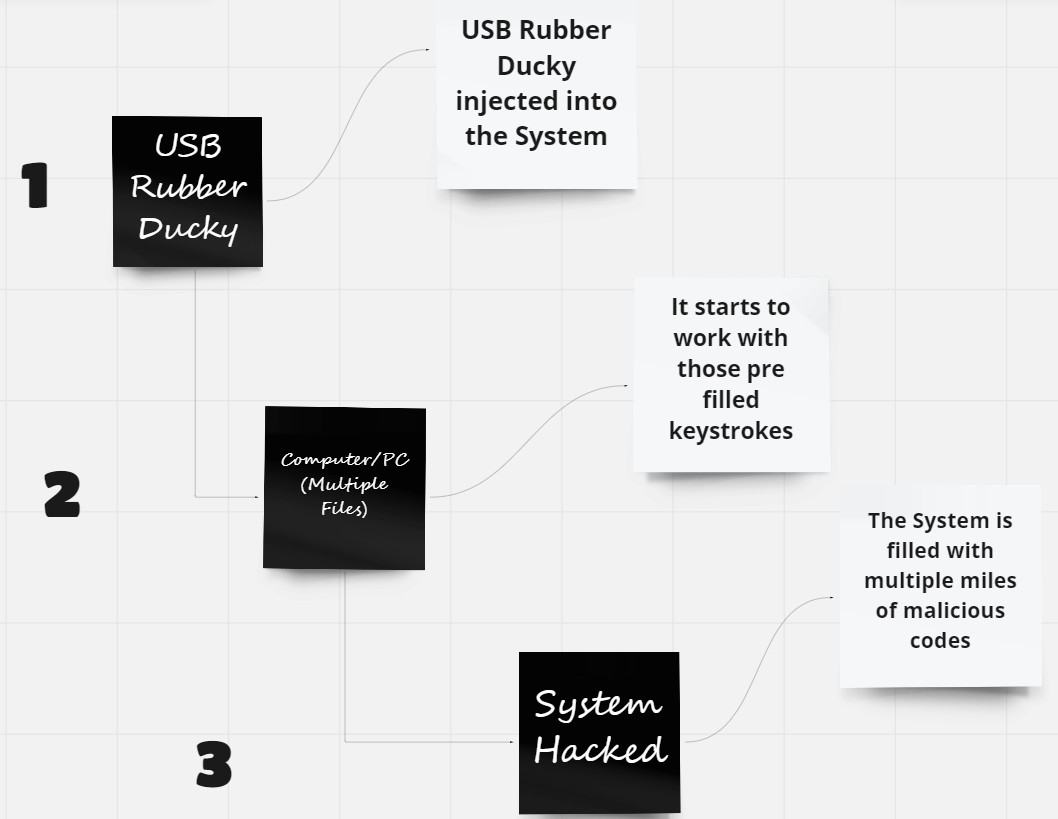
1. **For USB Rubber Ducky:**

The increase of external USB assault which is now a days a dangerous attack being developed as a testing tool in 2010, turns out malicious for common people as well as organization. It not only hacks the system but also avenge to steal the data either of the individual or sometimes of the whole organization. What is causing it and how does it happen? What should be a solution to such a HID device problem? USB Rubber Ducky is always set with the script to run venomous commands to complicate the situation for the user to handle it.

The Detection of Ducky is not an easy task because it is a Human Interface Device (HID) as mentioned above. It shows some of the changes to your pc while injected in the system but as soon as its work finishes it sets everything to as normal as before it was in user’s interface. Those activities what Rubber Ducky do as soon as it is done are:

1. It closes all the windows with commands which are opened by it while injected and gets back normal.
2. It also Deletes all the terminal and the browsing history it used to hack or extort the precious confidential information from the pc so that user won’t be able to identify what actually happened in their absence to their System leading to confusing activities of pc.
3. And. After all that it makes the computer to get back into the normal state of it without any evidence keeping behind. Clearing all the evidence of doubt.
4. It has the script in it for itself by cleaning everything suspicious without letting the user to doubt.

It can be detected by the proposed work mentioned for this piece of assault changing the Era of Cyber Security filled with lots of AI and ML based intellectual solutions to resolve problem in this area.



**Figure 5:** Process diagram of problem USB Rubber Ducky.

This figure describes a brief how the problem takes place and the system gets hacked. These are just the short steps of the Rubber Ducky attack process. This is just said to be the block process of steps-by-step by which the attack goes. This process will change drastically and give a hike to the society of Cyber Nation which gives a proper sense of Security to the common people and different organizations which sought to stand in the cue but are resisted due to threat of these risks or assaults. These are becoming a barrier in the life of the growing properties either it is individual or company or an organization.



**Figure 6:** Graphical Problem Statement.

* 1. **Proposed Solution/ Work:**

An approach to develop an AI based In- Built software serves as Virtual Assistant using AI sub set ML’s algorithm and programming language C/C++ or Python. This will help in order to provide faster response against the attack/ assaults so that we can slow them, stop them as well protect our system from them. Here, using the supervised machine learning way to train algorithms and prepare a model which is trained to prosecute the process and classify the dataset required. A clear dataset is required to classify the next step to make it easier for the model prepared.

* **Algorithm for USB Rubber Ducky:**

Algorithm is a well and an organized way to solve the problem. For USB Rubber Ducky, a structural algorithm to show the solution proposed to solve the problem. The algorithm is mentioned below on the upcoming page which shows the step-by-step process of the work proposed for this problem is:

**Step 1:** Insert a pen drive in the pc through the USB port.

**Step 2:** As the drive enters the port the pc/system starts to beep (Alarm).

**Step 3:** The sound of the alarm beep goes from low to sound in order to inform theuser or can connect the user’s mobile to alert.

**Step 4:** And then, the virtual assistant In-built for the USB protection gets activated mutes the alarm.

**Step 5:** That will ask for the voice recognition and eye recognition too**.**

**Step 6:** If, the condition matches with the user’s pre-set information.

**Step 7:** It will move further to ask the user to fill a unique password set for this Software.

**Step 8:** Else, move back to the Step 2 and the drive on the system won’t work till.

**Step 9:** If, the step 7 succeeds and the “BAD USB” works.

**Step 10:** Than, the software slow-downs the process of those multiple files.

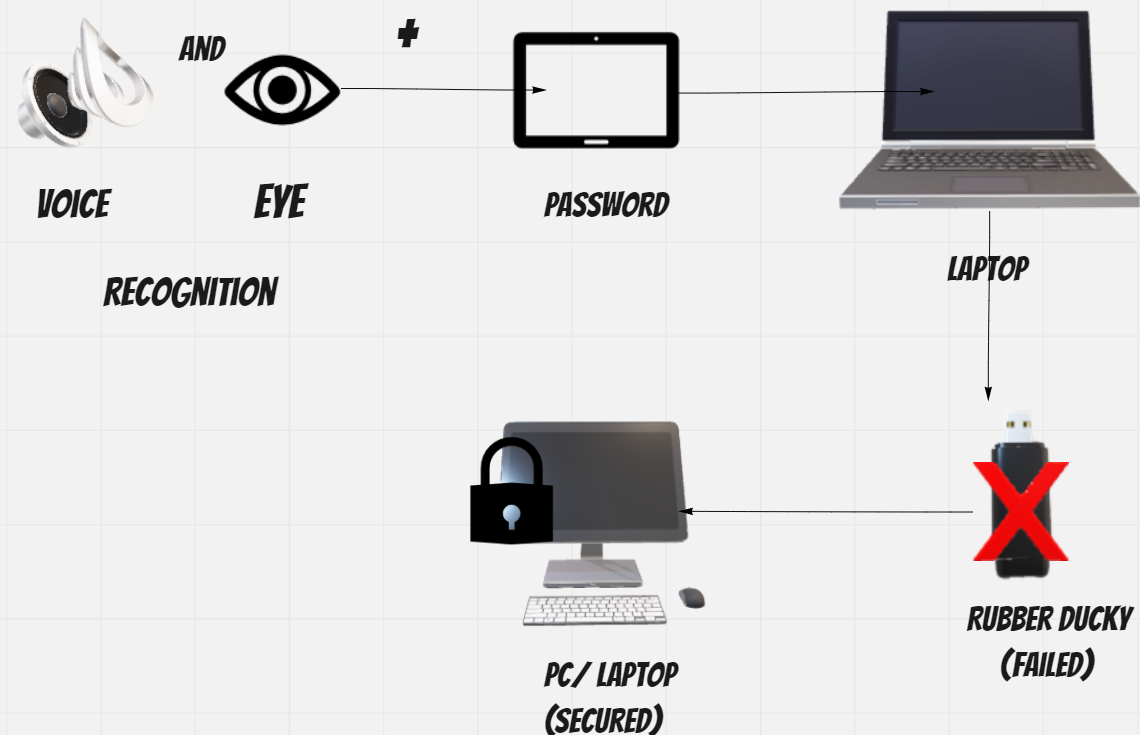
**Step 11:** And select the whole USB drive (Rubber Ducky), remove the multiple files of those rubber ducky script all at once.

**Step 12:** And automatically ejects the drive technically.

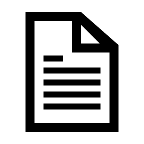
**Step 13:** Saved the confidential information!

**Result:**

This proposed work results into developing an In-built virtual software working as an assistant which firstly, prevents the work of the drive after entering the USB port and after that it slows down the process if it starts to proceed than, it will close all the multiple opened files of the malicious codes opened by the USB Rubber Ducky and after that starts to react in the response of the attack and soon after that ejects the drive automatically. This software will save the confidential data as well the system from getting hacked.



**Figure 7:** Brief Diagram of proposed work(result).

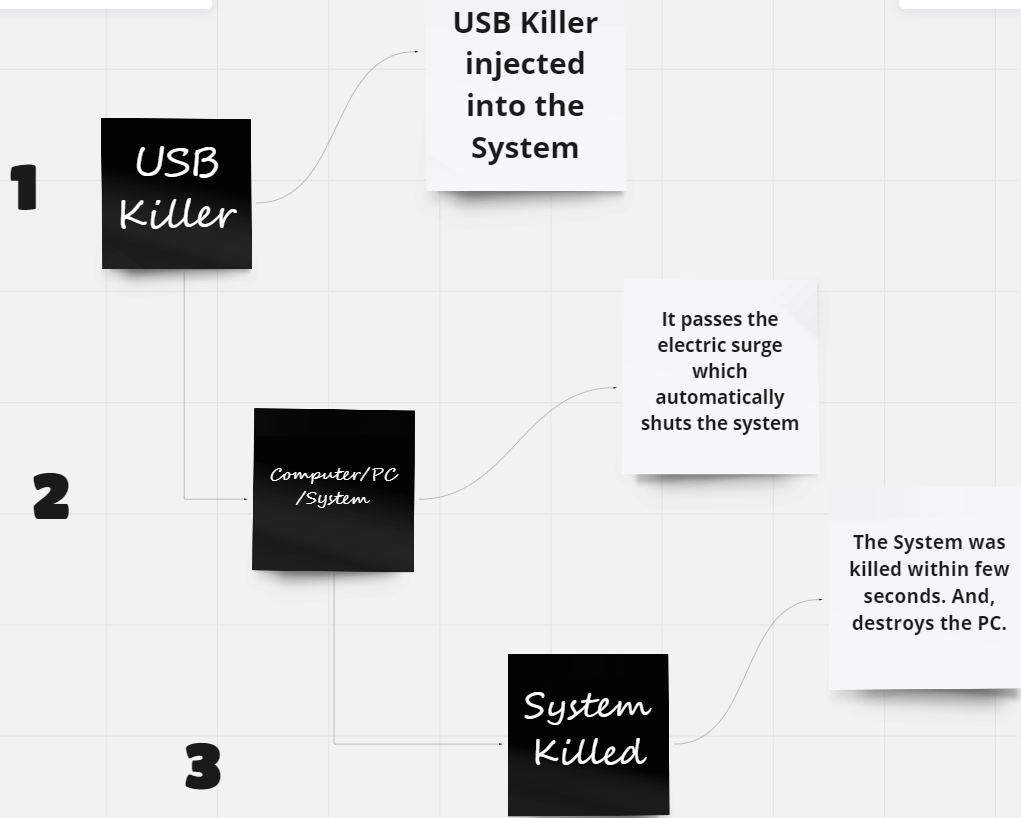


**Note:** USB Rubber Ducky and USB Killer both working is different but their purpose is totally same and that is actually to destroy the system and stealing the data. As they both are HID (Human Interface Device) which leads them to be undetectable. So, possibly they both might have almost the same solution which can help us resolve the problems. And, these tools being the HID might also have some similar activities to external USB Attacks. If it works, this will be a great help to the technology in order to make it easy and helpful to prevent our confidential data, system and privacy secure from frauds, assaults, attacks, terrorism and threats, etc. These can be a great aid for almost all of the USB attacks.

1. **For USB Killer:**

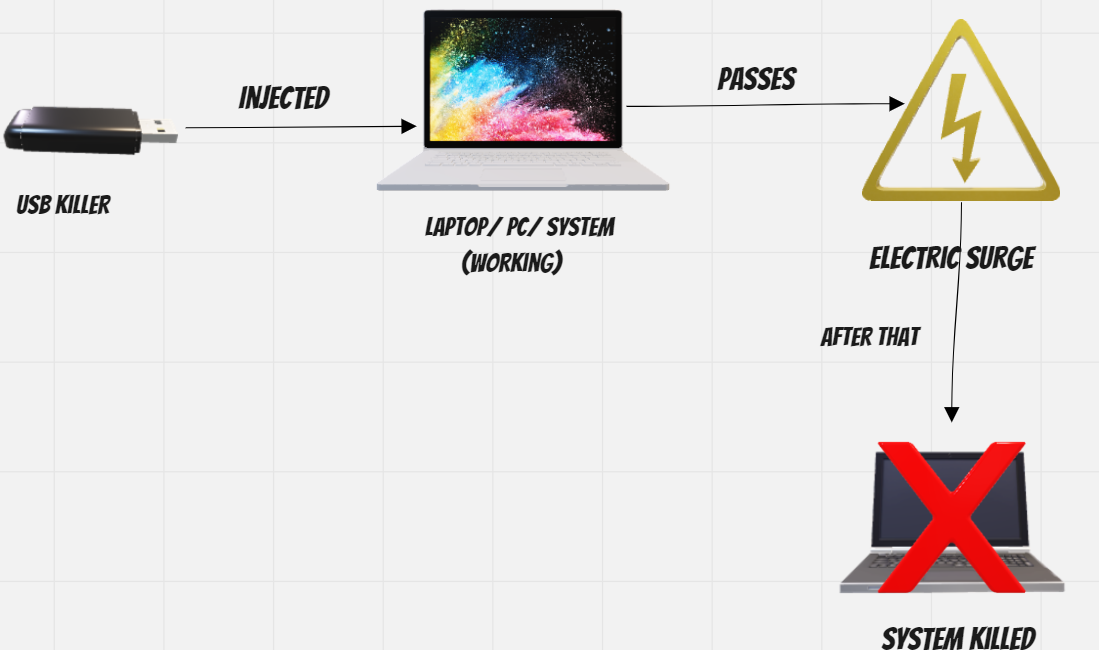
In the cyberworld, almost every day cyber-attacks or assaults either internal or external are observed even done under the table by the Hacker but are still observed anyways. In the same way, USB (external) attacks are also a part of it but are less discovered and known among the common society. Thus, the similar USB based electrical cum external assault was known in 2015, introduced by the person with the pen name “Dark Purple”. And, again a solid USB attack came into existence. Not only this, this was also mentioned the same as USB rubber ducky, a HID device as well the testing tool which turned to be a very cool hacking technique. This hacking tool, pass the 220V high power surge causing to immediately shut down the PC/Laptop/ system. Though, it cleans the whole data and confidential information from system in some case. Why is the process taking place and due to what circumstances? Is there any solution to this problem? How is this HID device being detected or could this problem be brought to an end?

USB killer is such a device which now a days also have an internal battery to make the attack offline accessible as well and more effective. This is how all the attacks are now getting more and more advance. Also, these HID devices make trouble by being unrecognized by the user. These attack through the USB port by just having the same outlook as normal pen drive. Are these HID devices safe to use after countering these types of attacks for common users? This becomes difficult for them to use any such USB drive again. These attacks are unknown. So, that’s why we tend to try for the solution of these external USB attacks causing frauds, threats and assaults.



**Figure 8:** Process diagram of problem USB Killer.

The Context above shows the process of the USB killer working as soon as it enters the USB port of the system and immediately destroys the device i.e., kills the device with a heavy electric surge of almost negative 200V which is devastating as a Kill.

****

**Figure 9:** Graphical Problem Statement.

* 1. **Proposed Solution/ Work:**

After analysing a lot, we approached to a solution that might help to solve the problem of protecting the electronic devices from being the target of this external USB attack. This is a very devastating attack for the device or the system. An evaluation made to develop an In-Built assistant cum software which seems similar to the project for the USB Rubber Ducky but the way of algorithm will be changed in it. This will be made using the ML’s Algorithm and models. Also, using the programming language C/C++/Python. This work will slow down the process of the attack as well destroys or stops the attack from proceeding any further. Here, unsupervised machine learning will be a way to train the algorithm to prepare a model which will be further trained to prosecute the process as unsupervised ML algorithm deals with the unlabelled data. So, to make the process clear.

* **Algorithm for USB Killer:**

Algorithm is set structural way of solving any problem quickly. It helps to solve the problem in a step-by-step method which decreases the chances of risk for any proposed solution. So, is for the USB Killer which is mentioned here. The algorithm is stated below:

**Step 1:** Insert a pen drive in the pc through the USB port.

**Step 2:** As the drive enters the port the pc/system starts to beep (Alarm).

**Step 3:** The sound of the alarm beep goes from low to sound in order to inform the user or can connect to the user’s mobile to alert.

**Step 4:** And then, the virtual assistant In-built for the USB protection gets activated mutes the alarm.

**Step 5:** That will ask for the voice recognition and eye recognition too**.**

**Step 6:** If, the condition matches with the user’s pre-set information.

**Step 7:** It will move further to ask the user to fill a unique password set for this Software.

**Step 8:** Else, move back to the Step 2 and the drive on the system won’t work till.

**Step 9:** If, the step 7 succeeds and the “BAD USB” works.

**Step 10:** The software starts to work faster than the USB works within few seconds.

**Step 11:** Software will than switches all the applications and folders on the screen so it will need the power to stay on.

**Step 12:** Than system will start to take the power of the drive leading it to consume all the battery of the drive.

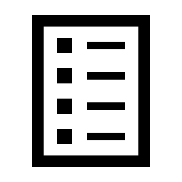
**Step 13:** Drive won’t work anymore.

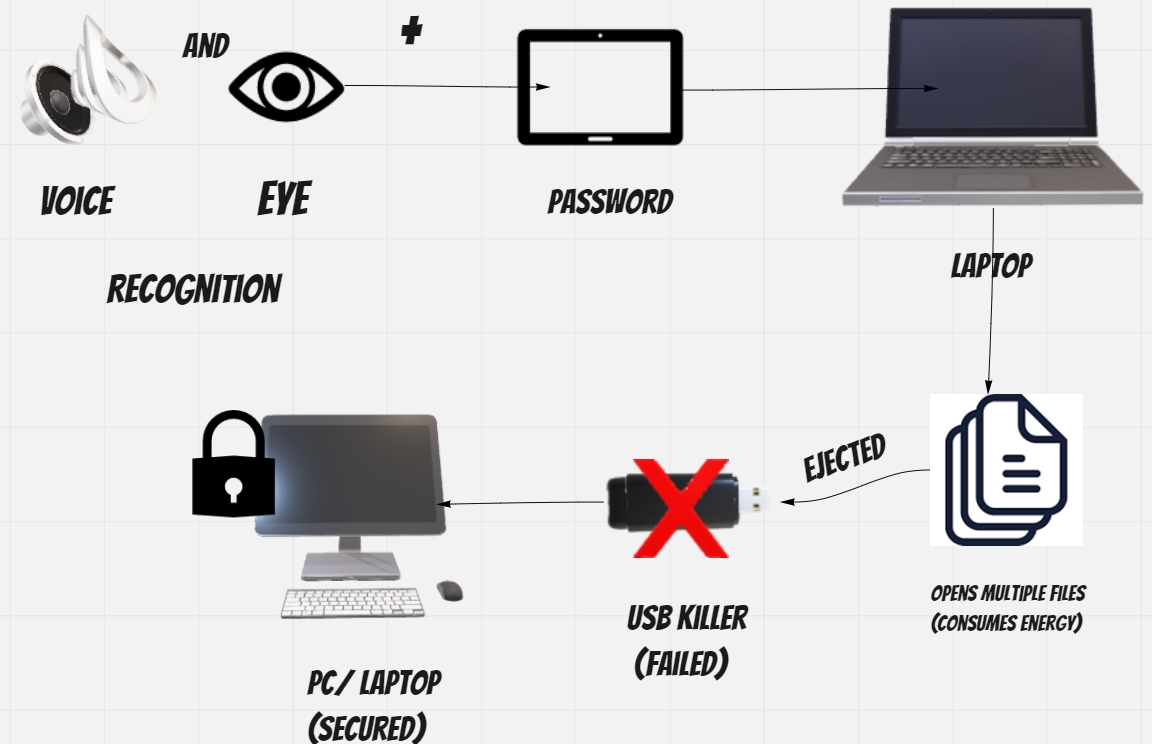
**Step 14:** If still works, then it will eject the USB technically immediately with veryquickResponse.

**Step 15:** USB ejected successfully!

**Result:**

The described plan results in building a trained model of an In-built virtual software who assists only the correct USB to enter in the port of the pc/system and let them proceed else will eject out the “BAD USB” or the wrong USB and will also safeguard from that. The expected response from this is to drain the battery of the USB Killer and is consumed by the PC so that it damages itself while attacking due to discharge of the battery. This makes the software reliable.

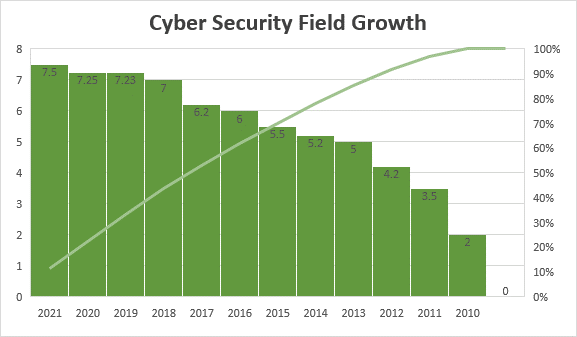
**Note:**

**** These results seem quite similar because of the similarity in the attack. USB assaults are really treacherous as they are very similar to simple looking USB pen drives and can’t be identified easily by anyone and amid that it creates a lot of trouble till the time user get to know. So, it is very necessary to be careful while using different types of USB’s, CD’s, DVD’s or any type of cable. As, any of them can be pirated. To rescue from these types of external assaults, the proposed work is an analytical approach we made.

**Figure 10:** Brief Diagram of Expected Result.

**Discussion**

Here in, we discussed about the cyberworld which is now a days full of assaults, attacks, threats, etc. This shows the importance of Cyber Security in the Cyber World and as well in the technology field. Assaults have held their tight grip on the devices. So, we have developed USB Rubber Ducky and USB Killer Algorithm which will help in preventing and stopping from taking irrelevant actions which could be harmful for our systems and are caused by the external or offline hacking gadgets or destroyers. So, ML’s supervised and unsupervised algorithms for USB Rubber Ducky and USB Killer. A hope or try to take Cyber Security to heights. This is the growth of field Cyber Security in past few years.

As the graph shown below states the increase of Cyber Security from 2010 to 2021:

**Figure 11:** Growth of Cyber Security field (2010-2021).

This figure shows the increase of the Cyber Security in the Cyber World from the years 2010 to 2021. This states that field of Cyber Security has extended vastly just after the Cyber-Crimes came to existence in this Cyber World. Cyber Security has provided lots of options for saving the society of common people who are unaware of these life threating assaults/attacks. This field proved its existence worthy in the upcoming world. A whole Cyber Security needs to be improved more in the upcoming years as it is the vast field and can help lots of problems to be heal. This is something which today’s as well as the new generation should be taught from their growing age to develop an asset to the country to settle the problems on their own with a creative solution and the generation should also be taught to aware their elders. Sometimes not elders can make children aware of the right and wrong. This will be helpful for the Nation to grow. These also should be kept in mind by them that any action should be made by taking note of their own safety as well the laws and ethics to make themselves safe and work legally. Any illegal action will be stated wrong and for that they need to face the strict consequences which will not be stated to innocence.

**Conclusion**

This is said that all in all security stands for “safety or security from anything” i.e., where safety meets the requirements of satisfaction. In the terms of technology also it means the same, to protect something confidential which is only possible when it meets the requirement to handle the problem. This is only what Cyber Security teaches us in all aspect to do and keep ourselves in safer and protective zone. But whatever is done to protect the data and important information it should be done in limits. That means, without crossing the limits of the legal actions, always keeping the cyber laws and ethics in mind we should take action. Under this process no illegal action should be take and also protect those laws from hindering by someone else. As safety is precious, that’s why for the protection we took an action of trying to develop a solution to these USB based attacks and two out of them are USB Rubber Ducky and USB Killer. For these, proposed work is given in this whole chapter with the help of different types of techniques as the techniques are improving and because of that technology is improving every day.

**Future Scope**

This field is full of growing scopes in the future. This is filled with lots of opportunities for the upcoming generation as far in the future. The study awareness is necessary about this field is very important and also about the Cyber laws and ethics. Not only the experts, we should also be updated about the cyber-attacks so that we will be attentive ever to any of the case. Everyone in this world should be well known about the categories of the viruses and thefts to prevent themselves from getting targeted from any such blunder. Cyber Security for youth is the mandatory thing because they are our upcoming generation. They should also know that which assault comes under which type such as the USB Rubber Ducky and USB Killer and USB drop attack, etc. are USB based attacks which comes under USB attacks of External Assaults. And, Phishing, spamming and etc. comes under the Internal Assaults.

These also shows the importance of Cybersecurity in the upcoming Cyber World. This field have created a hike all around the world and out of them some of the scopes are only mentioned here. The Future scopes in this field are so many that our next generation can choose to be as are mentioned in here:

1. CEH (Certified Ethical Hacker)
2. Application System Security
3. Information Security Analyst
4. Network Security Analyst
5. IOT security In charge

And many more are the scopes that we can see in this field as it is in so much of demand because of its speedy growth and due to this it led to the increase in demand of the employees.

The Future scope of the proposed solutions will be helpful for everyone in directing the detection of the GOOD or BAD USB making it to act as quick as possible for the reaction to work so that it can help the user to save their system and the software will take action quickly to resolve it and eject the USB technically to not let that BAD USB make any vulnerable activity possible and stops the task doing on the stop right there. Which is an effective task taking place itself by protecting the main objective of the Cyber Security.

**Abbreviations**

**A**

1. Artificial Intelligence (AI)

**C**

1. Certified Ethical Hacker (CEH)

**D**

1. Defense Research and Development Organization (DRDO)

**G**

1. General Public License (GPL)

**H**

1. Human Interface Device (HID)

**I**

1. Internet of Things (IOT)
2. Information Technology (IT)

**M**

1. Machine Learning (ML)

**N**

1. National Crime Records Bureau (NCRB)

**O**

1. Operating System (O/S)
2. Objective (Obj.)

**T**

1. Technique (Tech.)

**U**

1. Universal Serial Bus (USB)

**References**

[1]. A.S.M. Kayes,Alex Neg, Hamed Alqahtani, Iqbal H.Sarker (2021) ‘Cybersecurity data science: an overview from machine learning perspective.’

[2]. Pengrui Liu, Wei Wang, Xiangrui Xu (2022) ‘Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives.’

[3] Kathleen M.Carley, Lt.Col.David M.Beskow (2019) ‘Social Cybersecurity: An Emerging National Security Requirement’

[4]**.** E. Dilipraj (2014) ‘India’s Cybersecurity 2013: A Review’

[5] Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Miss. Sonali Mayekar (2021) ‘Era of Cyber Security’

[6]. Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Adnan Bukhari (2021) ‘A Survey on Cyber Security.’

[7] Cristopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey (2017), International Data Privacy Law, Vol.7, No.2, ‘The rise of cybersecurity and its impacts on data protection.’

[8] Zuoguang Wang, Hongsong Zhu, Peipei Liu and Limin Sun (2021), ‘Social Engineering in Cybersecurity: a domain ontology and knowledge graph application examples.’

[9] Mr. V. Harsha Vardhan, Y. Poornima (2017), ‘Cyber Security Issues and Challenges in India.’ International Journal of Scientific and Engineering Research, Volume 8.

[10] G. Nikhita Reddy, G. J. Ugander Reddy (2014), ‘A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies.’

[11] Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupkar (2021), ‘Research Paper on Cyber Security.’

[12] Ahmed Reda Alzighaibi (2021), ‘Cyber Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment.’

[13] Jelena Mirkovic, Terry Benzel (2012), ‘Teaching Cybersecurity with Deter Lab.’ Copublished by IEEE Computer and Reliability Societies.

[14] Jisha M M (2015), ‘Privacy Preservation in Data Mining with Cyber Security.’

[15] Cheng Gao, Xuan Zhang, Hui Liu (2021), ‘Data and Knowledge- driven named entity recognition for cybersecurity.’

[16] Bridges R, Jones C, MD.lannacone KT, Goodallj(2013) Automatic labelng for entityextraction in cybersecurity.

[17] Hasan M, Islam, M., Zarif and Hasem (2019). Attack and inconsisitent detection in IOT sensors in IOT sites using ML approaches.

[18] Olga Angelopoulou, Seyedali Pourmoafi, Andrew Jones, Gaurav Sharma (2019), “Killing Your Device via USB Port”

[19] Alejandro Rodríguez Ocasio Master in Computer Science Advisor: Jeffrey Duffany, Ph.D. Electrical and Computer Engineering and Computer Science Department Polytechnic University of Puerto Rico, (2015), “Implementing USB Attacks with Microcontrollers”.

[20] Rezky Aulia Efendy, Ahmad Almaarif, Avon Budiono, Muhardi Saputra, (2019), “Exploring the Possibility of USB based Fork Bomb Attack on Windows Enviornment”.

[21] USB Killer- Wikepedia (online).

[22] Benjamin Cannoles, Ahmad Ghafarian, (2017), “Hacking Experiment Using USB Rubber Ducky Scripting.”