Cyber Crime Under the Future Technology and the Technical Ranges Against the Hackers

G.Pandiselvi[1], K.Rathna[2], S.Joney Babayal[3]

[1]Assistant professor Department of computer science, Ayya Nadar janaki Ammal college, Sivakasi.
[2,3]Department of computer Applications, Ayya Nadar janaki Ammal college, Sivakasi.

Abstract:
The cyber crime means the data can theft that it undergone through out the world. Now a days the data that is more important than any other thing in the world. Cyber crime that is theft of data is more popularized on the world. By using our data, a information that we can access in anywhere of the world. Our personal data is the most important thing in the world the more and more both the positive and negative things of hackings are there in the world under the circumstances. To the world is moving on through the negative things of hacking. There is also an positive side of hacking. These positive thing of hacking not at all about theft it is just checking the way of security region. All digital data created, replicated or consumed is growing by a factor of 30, doubling every two years. By 2020, there will be over 40 trillion gigabytes of digital data or 5200 gigabytes for every person on earth. The more data you produce and store, the more organized crime is ready to ingest. Now a day's 24/7 online lifestyle gives enormous opportunities to reach anyone from anywhere but this gives chances to cyber criminals. Cyber criminals use big data to learn more about infected machines, breached databases and compromised information systems that opposes the human life. This means that hacking makes the AI to become an enemy of human world

Keywords: cyber security, robotics, AI hacking, cyber crime, hacking, data security, data protection, big data challenges on security, handling of big data.

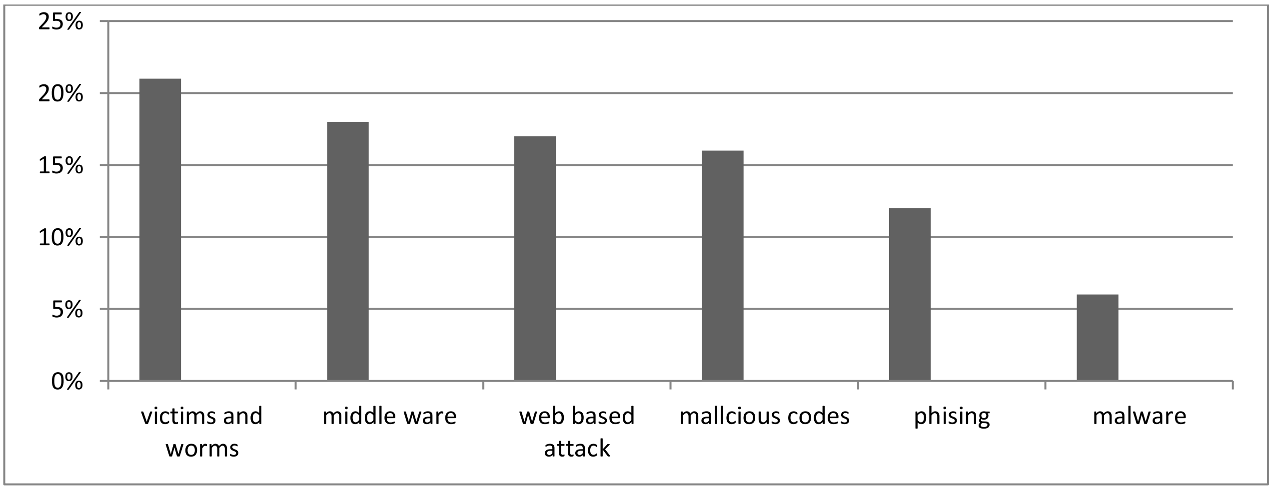
Introduction:
The security of data from hackers is known as cyber security this cyber security is executed in big data is hard to handle. A big data is nothing but a vast amount of data that it contains large amount of enormous information even of end users. Those are the user they cannot knew about the hacking of their data.One of the biggest threat of technological warfare is that no one can really predict the time and source of the miscreant activity. It can be remotely initiated, and a lot of times the repercussion of the infringement is only realized after a considerable damage. Although, respective Government of worlds nation are spending a great deal of resources and effort to protect their data and information from falling into wrong hands, the onslaught of social media porches namely Facebook, Twitter, YouTube and emergence of non-profit media organizations such as the WikiLeaks, who have a track record of exposing undisclosed Government information on public domain are making such efforts difficult. These trends are posing a threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information on the World Wide Web.

The data hacked from the user involves many crime regions that makes the cyber criminals to get lots of money from those data and it also gives the thrilling experience for the criminals. Such criminals makes our works to be loses because the viruses and malwares etc. In the part of the robots means AI makes our works easily even though it is let it for an military, army and navy forces. Thosethings saves the human from the dangerous hazards The machine that gets the full attraction and attention of the world then the human evolves the study of robotics and research makes dangerous to the human world they sustain.

cyber crime and security issues:

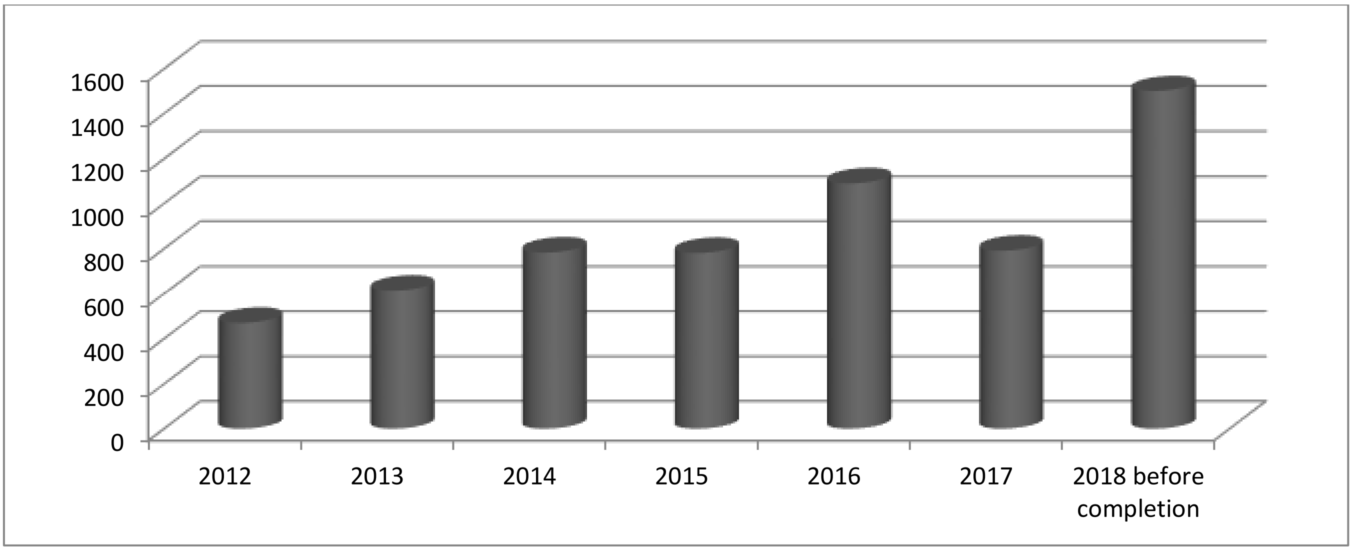
The cyber crimethat are undergone through some of the unrelated things of the world. So the hacking that means the act that can be taken as places by some of the activities. So some of the are **[i] victims and worms** those are the things victims are the unknown persons who has taken place some unwanted activities like theft the data of the user and worms are the unwanted software like the Trojan horse like theft related items. **[ii] Man in the middle attack** is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. **[iii] Web based attack** is that hackers can easily injects the malware predominantly through the website means majorly on internet is also known as cross site scripting. **[iv] Drive by attack or malicious attack** means hackers creates a content with exploit blocks vulenerabily needs to carry this downloaded attack they skillfully handles this attack**.[v]Phishing** is a fraudulent activity to obtain the sensitive information such as the user names, password and credit card details by disguising as a trust worthy entity in an electronic communication. **[v] Malware** it is a software designed on computers it does some of the damages to the computer they have an target to perform some of the tasks on the computer and take forms to execute the codes. **[vi] Denial of service DOS attack** is that the perpetrator seeks to make a machine or network resources unavailable to its intended user by distributing the host network services through the internet. **[vi] SQL injection attack** is the attack where the malicious SQL code for backend database manipulation to access the information that intended not to be displayed may be an secret pin number. The operation also might be possible on the sytems.

According to the above definitions the malware may be attacked as might as possible for the workings.



Even though the crimes are done on the different ranges the securities and restrictions are so tight for the usages some of the security undergone are **[i] Access control**is a key duty of a security guard is to control the **access** and egress to a facility or area. The purpose of controlling access and egress is to ensure that only authorized personnel, vehicles, and materials are allowed to enter, move within, and leave the facility. [ii] **Anti-key loggeroranti–keystroke logger** is a type of software specifically designed for the detection of keystrokes software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. [iii]**Antimalware** is a type of software program designed to prevent, detect and remove malicious software on IT systems, as well as individual computing devices. **[iv] Anti-spyware** software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. Detection may be either rules-based or based on downloaded definition files that identify currently active spyware programs. **[v] Anti-tamper**software is software which makes it harder for an attacker to modify it. There are no provably secure software anti-tampering methods. thus, the field is an arms race between attackers and software anti-tampering technologies. **[vi]Antivirus software** sometimes known as anti-malware software, is designed to detect, prevent and take action to disarm or remove malicious software from your computer such as viruses, worms and Trojan horses. It may also prevent or remove unwanted spyware and adware in addition to other types of malicious programs**. [vii]Cryptographic software** is a thing that is aencryption software is a type of security program that enables encryption and decryption of a data stream at rest or in transit. It enables the encryption of the content of a data object, file, network packet or application, so that it is secure and unviewable by unauthorized users.

It may works for an several ways the crime rate always in an increasing rate that it shows that as much made a normal persons to work for an worst activities like an hacking activities the statistics are given below according to the year database



Related works of cyber cell in India according to law

Mr.DhirenSehgal who explains about cyber crime and Indian cells against cyber crime. The cyber crime cells are the one track solution towards combatting and trackling those cyber crime. Now an act of the cyber crime is punishable criminal act that may be includes acts of online stalking, online banking or an credit card usage ,hacking and proliferating software viruses. These cyber crime cells are the brain children of the criminals investigating departments of cities in India and have been opened under these departments only to handle the issues of internet related criminal activity. This computer and internet based crimes are governed under the Information Technology act of 2000 and the act further penalizes such acts. We can arrange those cyber crime activity in two categories.

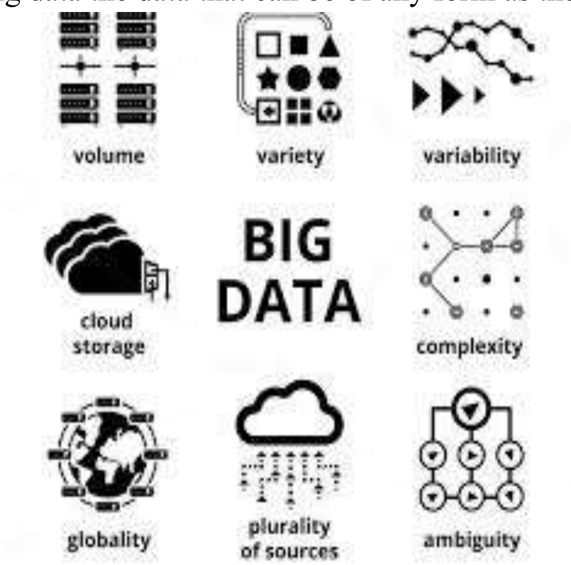
The computer as a target: The computers as a target by utilizing the personal computers to assault different computers . For example, that we may using the hacking tricks, viruses or the worm assaults, DOS assaults and so forth.

The PC as a weapon: The personal computers can act as a weapon by utilizing a PC to perpetrate and commit actual and real world criminal activities. For example, Digital Terrorism, IPR infringement, credit card scams, EFT cheats, pornography and so on.

According to the information technology act of India, when a cyber crime has been carried out, it has a worldwide purview and jurisdiction. Then the further technological assements are recorded in crime cell of all cities. A person gives a complaint by giving their correct personal details those activities are watched by cyber cell. In the hacking event data accompanied as i) logs of recorded in the server to look for the evidence of theft .ii) A duplicate of the hacked site page as a soft copy format and in addition printed version format, if casualty's site is destroyed. If information and data are lost or traded through the server or PC or another system network, then the soft copy of the original information and soft copy of original information. iii) Subtle details and information regarding access and control of the component hacked that is who had access to the PC or mail of the incident. iv) List of suspects if the reason is having any suicion on anybody. v) All applicable and relevant data prompting the response after inquires leading to the queries.

Challenges and Opportunities of Big Data:

According to the view of the big data the cyber security that can be of viewed as a great thing to show the developments. From the big data the data that can be of any form as the variety is given below.



[1] In the era of big data, awareness is the first line of defense against cybercrime. As one recent survey revealed, most cyber security, professionals know that they need to worry about big data, but they do not always clearly understand what itmeans. [2] Organizations should integrate customized processes and technical solutions geared to their specific risks and requirements to collect process, store, analyze and sharedata. [3] Integrating big data analytics into a solid infrastructure to provide and develop security solutions is essential – as is employing an expert IT staff to deploythem. [4] Strengthening cyber

security teams with highly skilled data scientists and analytics experts may become increasinglyessential. [5] Future investments in technology should lean toward flexible, analytics-based solutions that can change as business requirements and security threatsevolve.

View of robotics and working model with the importance of security:

Robotics and Artificial Intelligence both are huge fields in themselves and have a huge potential of future works done on the world. As the comments above suggest there can be a lots of research topics are there for advanced studies in robotics and artificial intelligence. Some of these in my opinion that could be

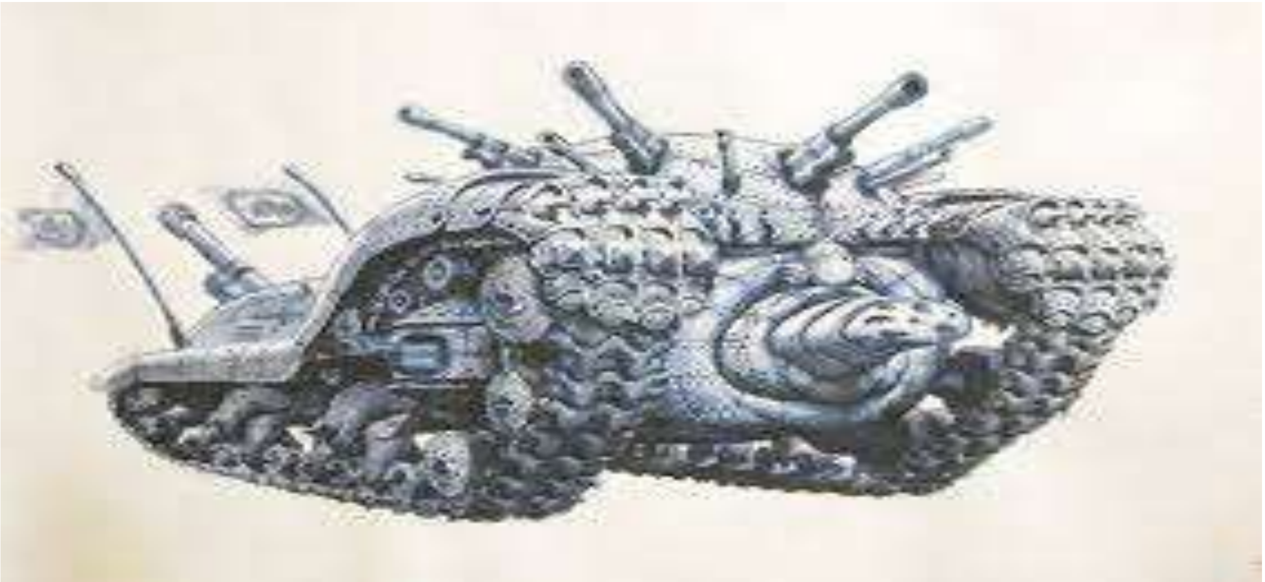
1. Reasoning and knowledge representation of problems
2. Behavior planning of robots
3. Human and robot interaction
4. Interactions of robots with brain
5. Computational models for communication
6. Learning of humans
7. Planning and recognition of things
8. Decision making process
9. Motion and path planning
10. Robotics vision

According to the robotics vision research held seriously to discover about to done the works of the human begin and also other than human works. If may be death in the border of navy forces loss of humans life that can be of reduced. The robots works like human and thing with intelligence other than the human begin and make right choice on the critical situation. The robotics works are well and good it is about the controller who robots to work. Assume that a hacker may operates this for the bad thing it becomes major hazards for the world. So that's why we mean that the cyber security is important thing for the whole world. From the law of the world will might be direct humanity into an acceptable future. The agents of change go unnamed for those who have yet to read it. [1] A robot may not harm humanity, or by inaction, allow humanity to come to harm. [2] A robot may not injure a human begin or , through inaction, allow a human, except when required to do so in order to prevent greater harm to humanity itself. [3] A robot must obey any orders given to it by human begins, except where such orders would conflict with the first law or cause greater harm to humanity itself. [4] A robot must protect its own existence as long as such protection does not conflict with the first or second law or causes greater harm to humanity itself.

A) Robotic vision:

US Mechatronics has produced a working automated sentry gun and is currently developing it further for commercial and military use. MIDARS, a four-wheeled robot outfitted with several cameras, radar, and possibly a firearm, that automatically performs random or preprogrammed patrols around a military base or other government installation. It alerts a human overseer when it detects movement in unauthorized areas, or other programmed conditions. The operator can then instruct the robot to ignore the event, or take over remote control to deal with an intruder, or to get better camera views of an emergency. The robot would also regularly scan radio frequency identification tags (RFID) placed on stored inventory as it passed and report any missing items. [1]Tactical Autonomous Combatant (TAC) units, described in Project Alpha study Unmanned Effects: Taking the Human out of the Loop. [2] Autonomous Rotorcraft

SniperSystem is an experimental robotic weapons system being developed by the U.S. Army since 2005.It consists of a remotely operated sniper rifle attached to an unmanned autonomous helicopter. It is intended for use in urban combat or for several other missions requiring snipers. Flight tests are scheduled to begin in summer 2009.[3] The "Mobile Autonomous Robot Software" research program was started in December 2003 by the Pentagon who purchased 15 Segways in an attempt to develop more advanced military robots. The program was part of a $26 million Pentagon program to develop software for autonomous systems.



B) Our major risks on that navy robots site:

Human rights groups and NGOs such as Human Rights Watch and the Campaign to Stop Killer Robots have started urging governments and the United Nations to issue policy to outlaw the development of so-called "lethal autonomous weapons systems" (LAWS). The United Kingdom opposed such campaigns, with the Foreign Office declaring that "international humanitarian law already provides sufficient regulation for this area". In July 2015, over 1,000 experts in artificial intelligence signed a letter calling for a ban on autonomous weapons. The letter was presented in Buenos Aires at the 24th International Joint Conference on Artificial Intelligence (IJCAI-15) and was co-signed by Stephen Hawking, Elon Musk, Steve Wozniak, Noam Chomsky, Skype co-founder Jaan Tallinn and Google DeepMind co-founder DemisHassabis, among others.

Proposed system and results of working:

In computing, a Trojan horse, or Trojan, is any malicious computer program which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious or by clicking on some fake advertisement on social media or anywhere else . Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.[6] Trojans may allow an attacker to access users personal information such as banking information, passwords, or personal identity. It can infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan. Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves. A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems. Users are typically tricked by some attractive social media adds who then directed to malicious website thereby loading and executing Trojans on their systems. Cyber-criminals use Trojans to spy on the victim user, gain illegal access to the system to extract sensitive data.

These actions can include:[1] Deletes Data, [2] Copies data, [3] Modifies Data,[4] Blocks Data, Disrupts the performance of the target computers or networks

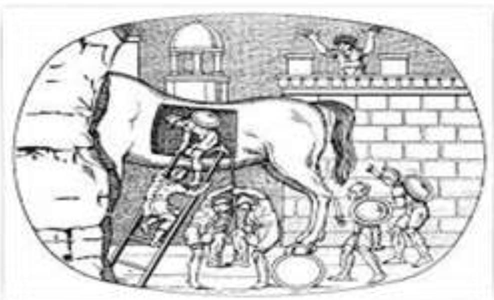
A) Types of Trojan Virus:

Trojan-Downloader: is a type of virus that downloads and installs other malware. [2]**Trojan-Droppers** are complex programs used by cyber criminals to install malware. Most antivirus programs do not detect droppers as malicious, and hence it is used to install viruses. [3]**Ransomware**- It is a type of Trojan (Trojan - ransom) that can encrypt the data on your computer/device. The cyber criminals who control this ransomware would demand a ransom for providing the decryption key. It is very difficult to recover the data without the decryption key. The WannaCry and Petya were recent ransomware attacks. Cyber security experts recommend users to follow a robust and systematic backup and recovery policy **[4]Trojan-Banker malware** programs steal account-related information related to card payments and online banking. **[5]Trojan-Rootkits** prevent detection of malware and malicious activities on the computer. These are sophisticated malware that provides control of the victim's device. Rootkits are also used to enroll the victim's device as part of a botnet. **[6]Trojan-Backdoor** is a popular type of Trojan. It creates a backdoor to allow cyber criminals to access the computer later on from remote using a remote access tool (RAT). As this Trojan provides complete control over the computer, it is a dangerous but commonly used Trojan.

There are many more types of trojans - some can send premium SMS, steal your instant messaging credentials, spy on system activities to capture keystroke data, steal email addresses and gaming credentials.

B) History:

This terminology occurs for the first time in a US Air Force report in 1974 on the analysis of vulnerability in computer systems. It was made popular by Ken Thompson in his 1983 Turing Award acceptance lecture "Reflections on Trusting Trust", To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust: the people who wrote the software.



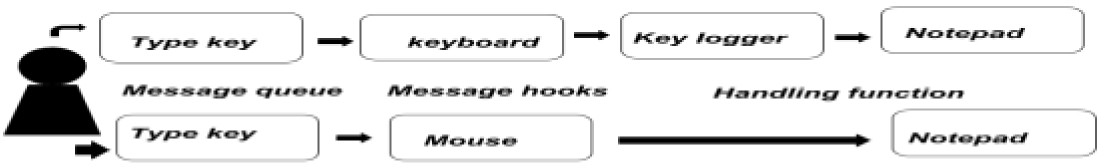
He mentioned that he knew about the possible existence of Trojan horses in a report on the security of Multics of which he was unfortunately unable to find a reference. However Paul Karger and Roger

Schell affirm that this is their above cited report.

C) Experimental works:

Our experimental works related to the Trojan horse is available on the net as a software after downloading thosetrojan horse software and this process that contains the key logger and screen shot program and those files are saved according to the certain time period within 50 seconds. The screen shots contains images of working when the screen changes images where taken the password and working details were stolen by the hackers. The key logger contains the text files that file contains the data related to the pressed keys that all keys are registered on the text files. By viewing the hackers also gets the details of idea of strategies by the way of getting the password and id values of the owner information.

1)Key logger challenge:



Virus name	Explaination
Black worm	Creates \windows\system32\About_Blackworm.C.txt
Nyxem	Targets the newyork mercantile exchange(Nymex)
My wife	Subjects surrounding mail attacks

According to the above images the key logger and screen shot can be identified on the view to know the information are identified after running those software.

vii) Performance and analyzes of cyber:

Performance and related issues made the cyber criminals develop those things in a different ways of the using. Some of the viruses that can attacks the computers are may be of different types by their working principles. Here we have explained the viruses with their name and definition of progress

According to the hacking many hacking cyber tools are available on the internet to perform some of the operation like theft the passwords make sure that the time consumption and the details that are needed for hacking was very important things to done the mater. Online hacking or cracking was most effective then the offline hacking of things some of them are

Tools	Target	Dictionary attack	Rainbow table	Brute force attack	Mode of usage
John and ripper	Password hashes	Yes	No	Yes	Offline
Ophcrack	NTLM hashes	No	Yes	No	Offline
Cain and able	NTLM hashes, my sql	Yes	Yes	Yes	Online and offline
Crowbar	Web authentication	Yes	No	Yes	Online
Lophtcrack	NTLM hashes, UNIX passwd files	Yes	No	Yes	Offline
Passcracking.com	MD5 hashes	Yes	Yes	No	Offline

Conclusion:

Finally, I conclude that the works done on the cyber security are growing larger and larger developing stage and also the crime rate was also in the increasing rate of working may the people falls on both things can work until their whole life. The crime rate makes the life of the people at last to the death and killer range. Not making most of the hackings a crime range of working many hackings possible done on their overall growth rate .The growth of the innovation and inventions makes the people to fall in hazards zone of hacking and crime think that equally developed crime results in the fall of working.The three V's of big data can be used to build a framework, which will integrate security issues, by design, using big data architecture.

References:

1. A. A. Cardenas, P. K. Manadhata, S. P.Rajan, Big Data Analytics for Security, IEEE Security & Privacy,11 (6), 2013, pp.74-76.
2. Enhancing Cyber security with Big Data: Challenges &OpportunitiesDecember 2, 2016 by Emmeline Short.
3. Elisa Bertino, E. (2014). Security with Privacy - Opportunities and Challenges
4. Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428
5. *"Dokumentnichtgefunden!".Federal Department of Justice and Police.Archived from the original on May 6, 2013.*
6. *"Swiss coder publicises government spy Trojan – Techworld.com". News.techworld.com. Retrieved 2014-01-26.*
7. *"German federal police use Trojan virus to evade phone encryption". DW.Retrieved 2018-04-14.*
8. BitDefender.comArchived August 8, 2009, at the Wayback Machine. Malware and Spam Survey *Datta, Ganesh. "What are Trojans?".SecurAid."Mega-Panzer"*
9. Solving Cyber Security Challenges using Big Data,PrajaktaJoglekar, NitinPise,International Journal of Computer Applications (0975– 8887)Volume 154–No.4, November 2016
10. Fonseca, M. Vieira and H. Madeira, "Evaluation of Web Security Mechanisms using

Vulnerability and Attack Injection," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1,2013.