1.1 INTRODUCTION:

Today’s enterprise networks are distributed to different geographical locations and applications are more centrally located, information represents the most important asset. With the growing number of data communication services, channels and available software applications, data are processed in large quantities and in a more efficient manner. This technological enhancement offers new flexible opportunities and also poses major security threats in the networks. These threats can be external or internal, external threats are divided as hacking, virus attack, Trojans, worms etc.

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user’s knowledge. A person writes the code, tests it to make sure it spreads properly and then releases it. A person also designs the virus's attack phase, and check it is functioning well according to its specifications. These can range from displaying irritating messages to deleting all the files on your computer. Viruses can have harmful side-effects, often called the payload, and are the aspect of most interest to users. Some of the things that viruses are capable of displaying different messages, denying all kinds of access, data thefts, changes in valuable data or files, deleting systems or any files, or it disable hardware.

All computer viruses are manmade. Today, trends of earliest computer viruses are attempted to hide evidence of their presence. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer virus damages the productivity of organization and organizations can lose billions of dollars. Viruses, as purely replicating entities, will not harm our system as long as they are coded properly. Any system damage resulting from a purely replicating virus happens because of bugs in the code that conflict with the system's configuration. In other words, a well-written virus that only contains code to infect programs will not damage our system.

Viruses have four essential characteristics. First, viruses are notable for the ability to replicate itself to infect computers, much like its biological counterpart. By replicating itself it is able to spread across computer systems and networks to infect as much as it possibly can. Second, before the virus can do anything, it must be
executed. If it cannot be executed, it is harmless. To get itself to replicate it hitched a ride by attaching itself to an executable program. It has to modify the program involved to also execute the virus code. The virus is usually attached to a common executable such as the operating system, which is automatically executed on startup. It may also attach itself to a commonly executed file that a specific company may use. Third, viruses do not just contain self-replicating code; they also contain what is called a payload. The payload is similar to a warhead on a missile; it is the side effect of the virus. The payload has the potential to be malicious, but it does not have to be. Lastly, the virus must be able to disguise itself before it is noticed by its side effects.

1.2 STATEMENT OF THE PROBLEM:

In last few years, with the extensive use of the Internet, networks, and email, computers have become more vulnerable to virus attacks and threats. A virus program has to be run before it can infect your computer. It can attach itself to other programs or hide in code that is run automatically when anybody opens certain types of files. It infects the file on a disk, in an email attachment, or in a download from the internet. As soon as we launch the file, the virus code runs. Then the virus can copy itself to other files or disks and this brings about changes in the computer.

Almost every week, new computer viruses are released into cyberspace. These programs spread as email attachments on computer. Therefore, an early detection and prevention mechanism is very important for the security of the computer. Anti-virus software is a critical link in overall security chain, protecting organization's computers from many types of viruses, including worms and Trojan horses. Using Anti-virus software is a good way to detect viruses and it is advisable to use Anti-virus software on network operating systems and workstations for adequate protection. The widespread use of broadband, WiFi, USB connections in home and small office networks has raised the need for proper Anti-virus software. Anti-virus software is specifically written to defend a system against the threats that malware presents. Anti-virus software may work differently and ranges from large security packages to small programs designed to handle a specific virus.

The large number of Anti-virus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. Therefore people have a choice of different types of Anti-virus i.e. both in the form of freeware software or licensed software. People frequently
change their Anti-virus software according to their liking and needs without evaluating the performance and capabilities of the various Anti-virus software available. Hence there is a need to find best Anti-virus software whose performance is good and also suitable for the specific needs of the users.

Therefore the study titled “A Study of Performance Evaluation of Anti-virus Software in Kolhapur and Sangli District”.

1.3 OBJECTIVES OF THE STUDY:
Researcher has conducted empirical research work on the basis of set objectives, the objectives are as follows;

1. To review the relevant literature of the study.
2. To study the popular Anti-virus software available in the market.
3. To identify the key performance indicators of an Anti-virus software.
4. To measure the performance of various Anti-virus software used by the different categories of users.
5. To suggest a model for benchmarking an Anti-virus software.
6. To study the financial investment made by the selected organizations in Anti-virus software in the selected districts.
7. To ascertain the percentage of licensed Anti-virus software users and trial Anti-virus software users.
8. To rank the various Anti-virus software available in the market on the basis of their performance.

1.4 HYPOTHESES:
The set hypotheses are tested and analyzed on the basis of the collected data and if found valid is accepted or otherwise rejected. Following are the hypotheses set by the study.

1. The key performance indicators considered by the users to evaluate the performance of Anti-virus software do not differ significantly among the different brands of Anti-virus software.
2. The quality of technical support provided to the customer differs significantly among the various Anti-virus software manufacture.
3. Investment made in Anti-virus software by different categories of users does not differ significantly.
The set hypotheses are tested on the basis data collection, analysis and interpretation.

1.5 RESEARCH METHODOLOGY:

For accomplishing the objectives, collection of both primary and secondary data is essential. Primary data is collected through survey method by administering a separate structured interview schedule to the identified respondents of Sangli and Kolhapur districts.

The methodology adopted is a mixture of literature review, document analysis such as government gazettes, interview with manager or officer in the organization, monthly and yearly reports from Anti-virus software and computer virus testing labs and survey of end users. The researcher has reviewed existing literature on Anti-virus software performance and viruses in India to understand the context and critical issues of the problem. This learning was supplemented with discussions with various users of computers such as students, managers, businessman’s, and other customers.

1.6 TOOLS USED FOR DATA COLLECTION:

Data Collection is an important aspect of any type of research study. Inaccurate data collection can impact the results of a study and ultimately lead to invalid results. Typical data collections strategies include:

1.6.1 Research Instruments:

As most of the literature showed, it is more effective if the multiple data gathering tools is used. Based on this assumption the researcher has used the combination of three popular data collection methods such as semi-structured interviews, questionnaires, and observations. The above mentioned objectives of the study are fulfilled by adopting these methods.

1.6.2 Primary Data:

The survey method is adopted to obtain the relevant information pertaining to the measure the performance of Anti-virus software in different organizations with the help of well structured questionnaire, interview schedule administer to distribute to officers.

1.6.2.1 Questionnaire: - Based on the objectives and in light of the review of related literature, the questionnaire is prepared and it was believed to be well responded as per the educational level of the respondents is concerned. The questions in the questionnaires comprised of both close-ended and open-ended
questions. The close-ended questions are used to easily categorize the responses gathered. The others are open-ended questions and their major purpose is to give opportunity to experts to express their feelings and perceptions related to the items without restriction.

1.6.2.2 Interviews: - Certain information required to fulfill a few objectives cannot be elicited with the help of the questionnaire alone. Interviews help to obtain relevant data that cannot be handled by questionnaire and essential to countercheck the information already obtained. To this end, a semi-structured interview is employed. In addition to making notes, unclear points can be elaborated due to the interview is done face to face. Taping of the interview is clarified with the person being interviewed. It also allows taking notes and doing follow-up questions, or deviating from the questionnaire, whenever that is required. This opened for more extensive exploration for open-ended interviews. Notes are taken throughout the interview. Each interview lasted for approximately 20 minutes.

1.6.2.3 Observations: - The researcher has assumed that observations provide an opportunity to collect data on a wide range of behaviors, to capture a great variety of interactions, and to openly explore the desired data or facts. By directly observing operations and activities, the researcher can develop a holistic perspective, i.e., an understanding of the context within which the public distribution system operates.

1.6.3 Secondary Data:

The secondary data is collected from existing published and unpublished literature which will be used for laying the conceptual framework. Other sources of secondary data are as follows:

(i) Documentary Data: Regular documents like annual reports, departmental publications of Anti-virus labs, worldwide computer virus database from internet and other records are used to collect the desired Information.

(ii) Training Material: For information pertaining to computerized information system, all the related training material and manuals are referred.

(iii) Library Sources: To collect information research journals, magazines are used.
1.6.4 Sample Design:

The study aims at collecting data from the users of Anti-virus software. Therefore; invariably all the people using a computer used an Anti-virus software. **Sampling Universe** – The entire users of computers comprises the universe for the study.

**1.6.4.1 Criteria for sample selections** – A study of data of users of Anti-virus software maintained by various Anti-virus software companies and their vendors, it has revealed that there are broadly 9-10 types of users, mentioned in bellow table no 1.1 [Table No.1.1: Sample size of districts, and Anti-virus Software Users]. Bellow table gives information about district wise Anti-virus software users in Sangli and Kolhapur districts of geographical scope considered for this study. Researcher undertaken study of these users of Anti-virus software, hence only registered user of Anti-virus software are considered for deciding sample and total 574 users out of 2708 are selected as samples.

- In this table, 3 out of 31 banks from Sangli district and 5 out of 45 from Kolhapur district are selected as a part of sample for the study.
- 10 out of 95 coaching classes from Sangli district and 14 out of 135 from Kolhapur district are selected as a part of sample for the study.
- 13 out of 127 educational institutes from Sangli district and 18 out of 180 from Kolhapur district are selected as a part of sample. In these selected educational institutes, 10 students from each educational institute are selected as respondents for the study. As for the student category random sampling method was adopted, thus total 310 students are selected as a part of sample size.
- 13 out of 130 government offices from Sangli district and 25 out of 248 from Kolhapur district are selected as a part of sample.
- 5 out of 51 Hotels, travel and tourism business firms from Sangli district and 17 out of 169 from Kolhapur district are selected as a part of sample.
- 11 out of 105 industries from Sangli district and 13 out of 126 from Kolhapur district are selected as a part of sample.
- 35 out of 345 internet cafes from Sangli district and 37 out of 370 from Kolhapur district are selected as a part of sample.
- 18 out of 182 professionals from Sangli district and 27 out of 369 from Kolhapur district are selected as a part of sample.
Therefore; the purposive quota sampling method was adopted for sample selection of these user categories.

**Table No.1.1: Sample size of districts, and Anti-virus Software Users**

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Anti-virus Software Users</th>
<th>Sangli District</th>
<th>Kolhapur District</th>
<th>Sample Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Total Units</td>
<td>Sample Units</td>
<td>Total Units</td>
</tr>
<tr>
<td>1</td>
<td>Banks</td>
<td>31</td>
<td>3</td>
<td>45</td>
</tr>
<tr>
<td>2</td>
<td>Coaching Classes</td>
<td>95</td>
<td>10</td>
<td>135</td>
</tr>
<tr>
<td>3</td>
<td>Educational Institutions</td>
<td>127</td>
<td>13</td>
<td>180</td>
</tr>
<tr>
<td>4</td>
<td>Government Office</td>
<td>130</td>
<td>13</td>
<td>248</td>
</tr>
<tr>
<td>5</td>
<td>Hotel and Travel &amp; Tourism Businesses</td>
<td>51</td>
<td>5</td>
<td>169</td>
</tr>
<tr>
<td>6</td>
<td>Industry</td>
<td>105</td>
<td>11</td>
<td>126</td>
</tr>
<tr>
<td>7</td>
<td>Internet Cafés</td>
<td>345</td>
<td>35</td>
<td>370</td>
</tr>
<tr>
<td>8</td>
<td>Professionals</td>
<td>182</td>
<td>18</td>
<td>369</td>
</tr>
<tr>
<td>9</td>
<td>Students</td>
<td>-</td>
<td>130</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td><strong>1066</strong></td>
<td><strong>238 [10%]</strong></td>
<td><strong>1642</strong></td>
</tr>
</tbody>
</table>

1.7 PERIOD COVERED IN YEARS:

Researcher has covered time period for the research work from 2009-10 to 2012-13 i.e., Three years because to consider the major practices in the area of Anti-virus software in selected organization.

1.8 SCORING PATTERN:

In the questionnaire some of the questions included in five points Likert type viz. \[1 = \text{Neutral}, 2 = \text{Poor}, \ 3 = \text{Fair}, 4 = \text{Good}, 5 = \text{Excellent}\] scoring pattern from Low to High level satisfaction, the respondents were asked to rate their level of satisfaction.
1.9 STATISTICAL ANALYSIS:

The percentage and average method was used for data analysis of the selected organization. The researcher has analyzed the raw data with the use of Microsoft Excel and different statistical methods like SPSS. The raw data is analyzed with the help of software prototype model which is developed on the basis of their performance.

1.10 SIGNIFICANCE OF THE STUDY:

Every company’s data is most valuable asset and must be treated as such. There are thousands of different viruses enters with improving its features every day in the market. In order to prevent data, many organization come forward and designed network security tools and Anti-virus packages. Anti-virus packages are mainly used to safeguard. Anti-virus software is class of program that reaches a hard drives and floppy disk, pen drives for any known or potential viruses. It runs random access of memory of a computer. Anti-virus packages are mainly used to prevent and remove the viruses, Trojans, worms etc, where as firewalls are used to monitor incoming and outgoing connections. Computers are used extensively to process the data and to provide information for decision making therefore it is necessary to control its use. Due to organizational cost of data loss, cost of incorrect decision making, and value of computer software hardware organisations suffer a major loss therefore the integrity of data and information must be maintained.

There are number of Anti-virus software venders in today’s market to remove the different computer virus. No one Anti-virus software can find or detect all types’ viruses and user cannot use more than one Anti-virus software at a time as it affects the performance of a computer system. Considering the vast scope of collecting data, only Kolhapur and Sangli District has selected for the study. The survey has conducted from major organizations like Nationalized and co-operative Banks, Insurance companies, Government offices, Universities, colleges, private industries, business etc. Detail information is collected through filing up questionnaire from each organization. Received data is analyzed with the help of statistical tools available. From this study it can suggest which Anti-virus software is suitable to particular area.
1.11 SCOPE OF THE STUDY:

- **Geographical Scope**: This study is confined to the district of Sangli and Kolhapur in Maharashtra state.
- **Topical Scope**: The focus of this study is on performance of existing Anti-virus software in the Sangli and Kolhapur district.
- **Analytical Scope**: The data collected as part of the study is analyzed to fulfill the objectives and test the hypotheses.
- **Functional Scope**: This research study covers the different key performance indicators that make Anti-virus software effective.

1.12 LIMITATIONS OF THE STUDY:

The work was started by visiting the owner, manager and end user of different organizations. In first few visits, general information was collected. The researcher has observed following limitations during research work:

1. It was very difficult situation to get an appointment of the officers and convey them to the importance of the research work.
2. The most of organization like banks, hospitals, owners were not interested to accept the questionnaire and discuss the issues due to fear.
3. Some respondents were hesitating to provide information due to secrecy of data and records.
4. Some respondents frequently change their Anti-virus software. Thus they not familiar with questions which are asked in questioner.

1.13 CHAPTER SCHEME:

A brief outline of the chapters of this thesis is as below:

**Chapter 1: Introduction and Research Methodology**
This chapter provides an introduction to the study, its need and importance, objectives of the study, hypotheses set out by the study, methodology employed and analytical tools used for analysis and testing of hypotheses. It also includes the scope of the study, limitations of study, chapter scheme and relevant literature reviewed.

**Chapter 2: Computer Virus Types**
This chapter gives an account of about history of internet, different data communication and exchange information medium, classification of computer virus
with computer virus name list with their category with examples. Working of computer virus is also described

Chapter 3: Symptoms and Prevention
This chapter covers the symptoms of different malware based on their classification i.e. software based symptoms, hardware based symptoms. It also describes the effect of normal windows function by attacking a malware. What are the effects on computer by infecting a malware to computer system and different ways to damage computer system? It also describes basic prevention mechanism taken by computer system when a malware is attack, different prevention tools are described in this chapter.

Chapter 4: Anti-virus Software
This chapter provides information evolution of Anti-virus software technology, objective of Anti-virus software, working of Anti-virus software. The brief profile of selected Anti-virus software is also described. It also covers the information about key performance indicator of Anti-virus software to measure the performance of Anti-virus software.

Chapter 5: Analysis and Interpretation of Data
In this chapter, the data collected from the survey of customer from different categories of users of the selected organizations is presented in tables and graphs and different statistical tools are used to draw inferences. The various hypotheses formulated by this study are also tested and presented in this chapter.

Chapter 6: Findings and Suggestions
This chapter summarizes the findings of the study and suggestions based on survey of different Anti-virus users. This chapter also covers the suggestions made to improve the effectiveness of the Anti-virus software which are used by the selected users. And suggest benchmark model for Anti-virus software industry how are developing different Anti-virus software’s packages and user manual for use of performance measurement tools.

Annexure

Bibliography
1.14 REVIEW OF LITERATURE:

[1] In this research article, the author has described a major computer security problem called a virus. Its ability to attach itself to other programs and cause them to become virus too. This research paper also introduces their potential for causing widespread damage to computer systems. Basic theoretical results are presented, and the infeasibility of viral defense in large classes of systems is shown defensive schemas are presented and several experiment are described.


[2] In this article, the author considers measures against computer viruses in a systematic way for Criteria for such steps are effectiveness, cost-efficiency, minimum disruption of normal operations, fast response and integration with general computer security. This paper author describe viruses and, in checklist form, those steps which should be considered by management when dealing with computer viruses. This paper concludes that Viruses are a fact of life. It is impossible to prevent viruses but the chances of an infection can be reduced by suitable policy. Costs incurred should be in line with the reduction in risk they offer. Viruses should be addressed formally as part of the computer security policy.

*Computer Viruses: A Management Perspective, MS Olivier, Centre for Advanced Computing and Decision Support (CSIR), 1990*

[3] In this research work, the author has described today's Anti-virus technology, based largely on analysis of existing viruses by human experts. In a few years, intelligent agents navigating through highly connected networks are likely to form an extremely fruitful medium for a new breed of viruses. At IBM, researcher are developing novel, biologically inspired Anti-virus techniques designed to prevent both today's and tomorrow's viruses. Here authors describe two of these: a neural network virus detector that learns to discriminate between infected and uninfected programs, and a computer immune system that identifies new viruses, analyzes them automatically, and uses the results of its analysis to detect and remove all copies of the virus that are present in the system.

*Biologically Inspired Defenses against Computer Viruses, Jeffrey O. Kephart, Gregory B. Sorkin, William C. Arnold, David M. Chess, Gerald J. Tesauro, and Steve R. White, Kephart, LSE Research Online, 1998*
In this research work, the author has examined a few open problems in computer virus research has resulted in a number of useful scientific and technological achievements. Techniques have been developed to help us estimate the safety and effectiveness of Anti-virus technology before it is deployed. Technology for dealing with known viruses has been very successful, and is being extended to deal with previously unknown viruses automatically. Yet there are still important research problems, the solutions to any of which significantly improve our ability to deal with the virus problems of the near future. The goal of this paper is to encourage clever people to work on these problems.

*Open Problems in Computer Virus Research, by Steve R. White, Virus Bulletin Conference, Oct 22, 1998*

This article provides insights and “safety instructions” designed to prevent Internet users from becoming Internet victims. Surfing the Internet is exciting, valuable, and very informative. Taking the time to identify potential dangers should be an integral component in any curriculum. All Internet users should be aware of these types of events and techniques. Educators who encourage Internet use among students may wish to include these precautions in their discussions. The insights and “safety instructions” discussed here have been designed to prevent Internet users from becoming Internet victims. Surfing the Internet is exciting, valuable, and very informative. Taking the time to identify potential dangers should be an integral component in all curriculums.

*Computer Crimes: How to Avoid Falling Victim, Dr. John A. Marshall, Journal of Industrial Technology, May 1999 to July 1999*

This article provides insights and “safety instructions” designed to prevent Internet users from becoming Internet victims. All Internet users should be aware of these types of events and techniques. Internet is used for getting valuable, and very informative. The five types of computer crimes present which are represent the types of challenges that face an information society dependent on computers. Criminal delinquents and ruthless con artists have developed acute computer skills, and are using them in a very creative manner.

*Computer crimes - how to avoid falling victim, Dr. John a. Marshall, journal of industrial technology, 1999*
In this research paper, the authors have described information about computer virus, different types of virus. It also describes different sources to get computer virus in to computer system, information about hoaxes and its factors. Also describe information about Anti-virus software and prevention method of attacking malware.

*Computer Virus - Technology Tips, Stanley R. Johnson IOWA State University, PM 1789j Revised, June 2000*

From this paper, the research has got knowledge about Malware and its different types. The researcher has examined, the history of viruses and look at the various techniques employed to propagate them. The researcher has recommended a comprehensive plan to combat viruses and reduce the damage of networks, in addition to the energy spent on the never-ending defense. Finally, the researcher has looked at future technologies as solutions towards fighting viruses. A basic understanding and awareness of how viruses work and which ones are “on the loose” will prevent users from continuing the domino effect of virus infections. Perhaps this game will never end but collaborative efforts by all computer users will serious impede the growth and damage caused by Malware.

*Living with Malware, Gary Wiggins, SANS Institute, 2001*

In this research article, the author has described that the virus problem will continue to evolve, just as it has for the past decade or so, and sometimes in unexpected directions. The explosive growth of the Internet and the rapid emergence of applications that disregard the traditional boundaries between computers threaten to increase the global spread rate of computer viruses by several orders of magnitude. The nature of computer viruses and their ability to propagate is on the cusp of a fundamental, qualitative change -- one that demands an equally fundamental change in the way we must defend against them. The new promising immune system is likely to be an important tool to control their spread for the foreseeable future. Home users, corporations and government entities need to seriously reconsider their security policies, and Anti-virus companies need to start working on the next generation of Anti-virus protection.

*Computer viruses: The threat today and the expected future, Xin Li, Avdelning, Institution Division, Department, 2003*
In this paper, the authors have focused on the detailed analysis of how long a flash worm might take to spread on the contemporary Internet. These analyses use simulations based on actual data about Internet latencies and observed packet delivery rates by worms. Flash worms can complete their spread extremely quickly—with most infections occurring in much less than a second for single packet UDP worms and only a few seconds for small TCP worms. Further, authors are analyzed the resiliency of flash worms to errors in their target lists and to automated worm containment defenses. Shallow trees are fairly resilient to list errors, but more vulnerable to containment defenses. Deep trees are very hard to contain, but need additional resiliency mechanisms to tolerate an imperfect list. Flash worms using deep trees can tolerate modest proportions of list errors or containment defenses.

*The Top Speed of Flash Worms, Stuart Staniford, David Moore, Vern Paxson, Nicholas Weaver, The Cooperative Association for Internet Data Analysis, 2004*

In this research paper, the author has described the information about viruses, types of viruses, other destructive programs. And also discuss some common ways for spread viruses into the system and how viruses affect your system, characteristic for compute virus infection to any target, information about real virus threats. There are some methods to protect your system. When designing security appropriate to your operation which areas are covered. Tasks performed by the Anti-virus software for preventing attack of computer virus.

*An Introduction to Computer Viruses (and Other Destructive Programs), White paper, McAfee - Network Security & Management, 2005*

This publication provides recommendations for improving an organization’s malware incident prevention measures. It also gives extensive recommendations for enhancing an organization’s existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and Rootkits. The recommendations encompass various transmission mechanisms, including network services and removable media.

[13] In this research article, the author has described the origin of computer virus and history of computer virus with most dangerous virus and some steps for protect against computer viruses. And also described computer viruses are mysterious and grab our attention. On the one hand, viruses show us how vulnerable we are. A properly engineered virus can have an amazing effect on the worldwide Internet. Viruses - both "traditional" viruses and the newer e-mail viruses - so that you can learn how they work and also understand how to protect yourself. Viruses in general are on the wane, but occasionally a person finds a new way to create one, and that's when they make the news. 

_Anatomy of Computer Viruses, Chuck Hauge, CPH Solutions, 2006_

[10] In this article, the authors have explained about different malicious code environments and discussed about the different types of viruses and worms, different characteristics of computer virus and detail about the various ways of virus, worm and their categories, propagation techniques and their differences, it also include case studies of Slammer and Blaster worms. In that case studies author explain how these worms are working.

_Seminar Report on Study of Viruses and Worms, H. Shravan Kumar, Prof. Bernard Menezes, Kanwal Rekhi School of Information Technology, IIT Bombay, 2006_

[11] In this research article, the author has described information about computer malware, types of malware. Computer malware has been a serious issue for many years and, it’s very likely to stay with us for a long time to come. There are many tools at our disposal, including excellent free ones, for arranging an effective defense and this will introduce you to the various dangers you might face in future together with easy methods for getting rid of them and restore your computer an healthy status. Each of the main malware categories are faced one by one by explaining what they do.

_A simple guide to Computer Viruses and other dangerous little programs - An Introduction to an Effective Defense, Roberto Dillon , International journal of law and technology, Program and Play - Roberto Dillon, 2007_

[12] In this research article, the author has described the importance of protecting our computer. If you have a computer that connects to the internet then protecting your computer is crucial. Your computer is not only prone to viruses, spyware and other
unwanted traffic including theft of information from your computer, but can also be used for criminal or spamming purposes by hackers. The different tips and techniques like installation of Anti-virus software firewall, browsers setting and other useful tips to protection of any computer from all types of malware, Internet Frauds and Scams, etc.

*Protecting Your Computer and Your Identity, Security Awareness, Office of Enterprise Security Dept. of Information Technology, 2007*

[13] In this research article, the author has described computer hard- and software evolve, there will be persons writing and distributing Malware to exploit security holes for their own interest. How Malware evolved from times when a computer virus was considered to be a myth until today, when Malware is a serious threat to everyone, tied to the history of computing hardware, and the Anti-virus community.

The primary distribution channel will stay the internet and the WWW. With the growing importance of online applications, it is necessary to defend these infrastructures with all possible means against Malware.

*Evolution! From Creeper to Storm, Robin Wielputz, Seminar on Malware, Bonn-Aachen International Center for Information Technology, 2007*

[14] In this research article, the author has described the concepts of web, three stages of internet growth i.e. web 1.0, web 2.0 and web 3.0. The internet is very useful for communication between two or more computer in various different places. In today’s world of extreme competition on the business front, information exchange and efficient communication is the need of the day. And also describe the comparison between web 1.0, web 2.0 and web 3.0. The comparison summaries that First web1.0 is about knowledge of all kinds get represented in a form that is interpretable both by people and machines. Second web 2.0 is about different forms of language in which knowledge is expressed begun to be interrelated and made interchangeable with each other. And web 3.0 is encoded in a semantic form; it becomes transparent and accessible at any time to a variety of reasoning engines.

*Comparative Study of Web 1.0, Web 2.0 and Web 3.0, Umesha Naik, D Shivalingaiah, International CALIBER-2008, 499 - 507*

[15] This research paper exhibits shared patterns for classification of malware. The diversity and amount of its variants severely undermine the effectiveness of classical
signature-based detection. Yet variants of malware families share typical behavioral patterns reflecting its origin and purpose. The main contribution of this paper is a learning-based approach to automatic classification of malware behavior. The key ideas of our approach are: (a) the incorporation of labels assigned by Anti-virus software to define classes for building discriminative models; (b) the use of string features describing specific behavioral patterns of malware; (c) automatic construction of discriminative models using learning algorithms and (d) identification of explanatory features of learned models by ranking behavioral patterns according to their weights.


[16] This article makes a brief introduction of the computer virus’ concept and characteristic and has enumerated some computer virus' typical symptom; introduced the treatment computer virus' method through the example. Some virus even can clean the hard disk or make the hard disk impossible to visit. Virus' biggest harm is enabling the entire network to sink into the paralysis. In the near future, the computer virus is reeking seriously, these virus is trying to close each kind of Anti-virus software and automatically download dozens kind of robber number wooden horse virus, and will bring the enormous los to the user. Look up and kill this virus is more difficult than “the panda to burn incense”. So, computer virus' preventing and controlling work appeared especially important.

Computer Virus Preventing and Controlling Method Discussion, ShenYanmei1, XieHong, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10), July 2010

[17] In this research article, the author has described the growth of Computer virus threat and home users are threatened by them, especially with the increasing dependence on computers to accomplish the vast verity of tasks in our modern lives. This paper describes definition of computer viruses, their nature, their history and development, and their different types is, computer virus writers nature, motivations and their perspective to legal and ethical issues is highlighted, to eliminate the threat of computer viruses is discussed. By comparing the increasing number of home users with the increasing number of computer viruses each year, we can easily realize the
growing threat of computer viruses towards home users. The increasing awareness of computer viruses and basic IT security principles will help home users to eliminate the threat of computer viruses.

*Computer Viruses as a Threat to Home Users, Dr. Waqar Ahmad, International Journal of Electrical & Computer Sciences IJECS, 2010*

[18] In this article, the author has discussed about viruses -- both "traditional" viruses and the newer e-mail viruses – so that you can learn how they work and also understand how to protect yourself. Viruses in general are on the wane, but occasionally a person finds a new way to create one, and that's when they make the news. And also he has discussed the most common infection types. Like virus, worms, Trojan. Working and prevention method of cold red and I love you virus are discusses.

*How Computer Viruses Work, Marshall Brain, Manitoba E-Association's, How stuff work, 2010*

[19] In this research article, the author has described the threats that computer viruses pose to research and development multi-user computer systems; it has attempted to tie those programs with other, usually simpler, programs that can have equally devastating effects. Although reports of malicious programs in general abound, no non-experimental computer viruses have been reported on mainframe systems. This paper has described several easily harmed methods in the research and development environment that malicious programs could exploit, and also discussed research underway to improve defenses against malicious logic. Noting that the number of people with access to mainframes is relatively small compared to the number with access to personal computers. Should an attacker use a computer virus or other malicious program, security mechanisms currently in use will be as effective as they are against other types of attacks.

*An Overview of Computer Viruses in a Research Environment, Matt Bishop, the Dartmouth Computer Science Research Symposium (CSRS2011), 2011*

[20] In this paper, the authors have focused on the growth in E-commerce, today’s open source nature of malware, the growing penetration of the Internet in respect to insecure connected PCs, are among the main driving factors of the scene. It includes different trends and techniques used for developing malware and a survey on how
these can be handled in an efficient manner. It also discussed about different issues related to malware starting first from the structural properties of the malware and its behavior which is necessary for analysis so as to able to defend them. At the end author discussed about the latest mitigation strategies which can detect the malware, latest techniques which are being used for the mitigation.


1.15 CONCLUSION:

On the basis of the evaluation of the literature reviewed which are mostly in the form of research articles in the field of computer Anti-virus software and solutions development for protection from malware it can be concluded as follows:

Most of the literature reviewed reveals that the earlier studies are related mainly to the different types of malware like virus, worms, Trojans etc. The different tips and techniques like installation of Anti-virus software firewall, browsers setting and other useful tips for protection of a computer system. Some of the research work is related to the latest mitigation strategies, which can detect the malware, latest techniques which are being used for the mitigation of viral attacks. While others have discussed the security mechanisms currently in use against malware, Internet Frauds and Scams, etc.

Therefore, critical gaps are apparent in the previous researches in the areas related to evaluation of the various Anti-virus software available in the market, measure the capabilities of each brand of Anti-virus software in protecting the computer system from the various types of malware and the evaluation of technology adopted in developing the Anti-virus software.

In view of the above issues the researcher has decided identify the parameters to measure the performance and capabilities of the various brands of Anti-virus software and to develop and suggest a benchmarking model for the various Anti-virus software.

REFERENCES

3. Stanley R. Johnson, Computer Virus - Technology Tips, IOWA State University, PM 1789 Revised, June 2000
4. Xin Li, Avdelning, Computer viruses: The threat today and the expected future, Institution Division, Department, 2003
5. Stuart Staniford, David Moore, Vern Paxson, Nicholas Weaver, The Top Speed of Flash Worms, The Cooperative Association for Internet Data Analysis, 2004
8. ShenYanmei1, XieHong, Computer Virus Preventing and Controlling Method Discussion, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS ’10), July 2010