CHAPTER VI
FINDINGS AND SUGGESTIONS

A. FINDINGS;

A: 6.1 Introductions:

The present study gives an insight into the use of Anti-virus software among the different categories of users. The observations and findings of this study are based on survey of users belonging to nine (9) different categories. The data thus generated is compiled and analyzed in the previous chapter, wherein interpretation and inferences are drawn there from. Based on this analysis, observations and findings related to the use of Anti-virus software are presented in this chapter.

A: 6.2 Findings common to all the Users:

1. It is observed that there are six different brands of Anti-virus software that are being used by the various categories of users in the selected area. The study reveals that NPAV and Quick Heal are the two most popular Anti-virus software brands being used by different categories of users. However it is also revealed that the Norton brand of Anti-virus software is used by majority of the banks on account of its reliability and dependability for secured transaction on the network. Quick Heal brand of Anti-virus software is being used by majority of the coaching classes, government offices, hotel and travel tourism businesses and the industries. Majority of users of NPAV brand are students, educational institutions and professionals.

2. During the study it is observed that ‘Home Edition’ type of Anti-virus software of all brands is being used by majority of the user [39.72%]. This type of Anti-virus software gives basic protection to the computer system. ‘Total Security’ type of Anti-virus software has the second highest number of users [37.11%]. It is also observed that total security type of Anti-virus software is being offered by majority of brands like Quick Heal, NPAV, Norton, McAfee, and Kaspersky.

3. The study reveals that the various type of Anti-virus software offered by each brand does not have uniform number of users except for the Norton ad Quick Heal Anti-virus software brands where all types of their Anti-virus software are used by its users in the Sangli and Kolhapur district. It is found that in case of AVG brand,
FINDINGS AND SUGGESTIONS

‘Home edition’ is the major type used with 76% and 50% users in Kolhapur and Sangli district respectively. In case of Kaspersky, ‘Home edition’ and ‘Total Security’ are major types with 66% users in Sangli and 63% in Kolhapur district. The home edition type of McAfee has 55% users in Sangli and 30% in Kolhapur while ‘total security’ type of the same brand has 35% users in Sangli and 46% users in Kolhapur district.

4. The study reveals that the majority of the users surveyed use licensed copy of Anti-virus software. However a sizeable percentage [28%] uses trial versions of Anti-virus software. Majority of the trial version users are internet cafés and students who would like to save on the cost of licensed fees and thus depend on trial version that are available free of cost.

5. The study reveals that the criteria adopted wile purchasing Anti-virus software comprises of four main factors namely price, brand name, after sales service and system security service provided. However it is seen that brand name of Anti-virus software and the price are two important factors that are being considered by the various category of user except for the banks rest all of the users [34.5%] are influenced by the price of Anti-virus software. Therefore the users of these two districts are fairly price conscious. It is also revealed that the customer category of banks does not considered price as an important factor wile taking purchase decision. This category considers the brand (reliability and dependability) and capability of Anti-virus software. Therefore the study also reveals that greater the need for transaction and information security or safety lesser is the consideration for cost.

6. It is found that the factors that influence the buying decision with respect to Anti-virus software comprise of price, brand name, after sale services, system security service provided. Whereas the importance given differs among the four factors for each brand. For AVG brand, system security services is the main consideration factor. In case of Kaspersky, McAfee, Norton and Quick Heal it is the brand name (reliability and dependability) that is considered while purchase these brands and in case of NPAV it is the price which influences the buying decision of the users.

7. The study reveals that the investment in Anti-virus software is directly proportional to importance of data and transaction processes. This is based on the finding that it is only the bank category which invests more than Rs. 2500/- per
year in an Anti-virus software system. The rest of the users invest less than Rs. 1000/- per year (58.8%) because their security needs are not as strong as that of a bank. Therefore it is clear that majority of users’ investment in Anti-virus software is low.

8. The district wise analysis of the investment made by the user also shows that it is the banks 60% in Kolhapur invest more than Rs. 2500/- per year and 66% of the banks in Sangli in between Rs. 1500/- to Rs. 2000/- per year in an Anti-virus software where as rest of the user categories invest less than Rs. 1000/- per year i.e. 59.8% in Kolhapur and 57.6% in Sangli district.

9. On the basis of data analysed, it is observed that majority of users (72.1%) use the Internet. It is the category of coaching classes, hotel travel and tourism business (1.39%), which is connected through a LAN where as all the banks and majority of internet cafés (80.5%) are connected to the internet through a LAN while only 5.5% of the users are not connected to the internet.

10. It is observed that majority of users (85%) connect some or the other external storage device to their computer. Therefore, use of external storage devices is very common among the various users of the two districts. Only 50% of the banks and 35% professionals are those who do not connect any external storage device to their computers. Therefore only a small percentage (15%) of the users has a minimal risk of being infected with any malware and therefore may not need an Anti-virus software. However majority of this percentage belongs to bank category which is connected through a LAN. Thus necessitating the use of Anti-virus software. Therefore almost all users need Anti-virus software.

11. It is observed that the ‘help support’ service provided by all the brands of Anti-virus software is good to fair. i.e. more than 82% of the respondents fall in this brackets. Therefore the help support service provided by all the brands of Anti-virus software is prompt and up to date. Among the brands, ‘help support’ service provided by Kaspersky is the best. Because all its users have rated this service provided by Kaspersky as excellent to fair. Hence it is clear that ‘help support’ service of Anti-virus software has to be satisfactory and above for reasons that are obvious. i.e. an Anti-virus software has to operate in very dynamic system, which is rendered unstable due to malware attack. Moreover the lists of malware in circulation keep growing by the day.
12. It is reveal that the ‘virus-definition-update’ service provided by all the brands is prompt and up to date. Majority of the respondent 55.7% have rated this service as good to excellent. Since virus definition update is an integral part of Anti-virus software i.e. because without updating new virus definition the Anti-virus software is unable to scan for new malware.

13. The study reveals that with the arrival of a new malware like virus, worm, Trojan etc. on the internet it is necessary for the Anti-virus software developers to be able to handle the malware by identifying it and getting rid of it. Therefore Anti-virus software developers need to update their code by using some new technology. This type of revision by the Anti-virus software developers is called as version update, which is an integral parts of Anti-virus software applications. Hence this feature of all the brands is above the satisfaction of the users.

14. It is found that the ‘on-access scanning’ capability is a most preferred aspect of Anti-virus software. I.e. specifically used to scan any secondary storage device. Therefore all the brands include this capability in their application. Majority of respondents are satisfied with this service provided by their Anti-virus software developer.

15. It is found that the ‘on-demand scanning’ capability is also a most preferred aspect of Anti-virus software. i.e. specifically used to scan a secondary storage devices. Therefore all the brands include this capability in their application. Majority of respondents are satisfied with this service provided by their Anti-virus software developer.

16. It is revealed by the study that ‘scheduled scanning’ service provided by all the brands of ranges from excellent to fair. The scheduled scanning service is very useful feature of Anti-virus software which can be enabled during the idle time of the computer system. Hence this feature is excepted by majority of the users. However it is observed that majority of users of Kaspersky brand are more than satisfied with scheduled scanning feature provided by their Anti-virus software provider. Where as in case of Quick Heal majority of its user (38.6%) have rated this feature as poor.

17. On the basis of the analysed data it is found that the ‘auto-clean infected file scanning’ feature provided by the different brands of Anti-virus software is excellent to good. Auto clean infected file scanning service is an integral part of
an Anti-virus software application that ensures protection from malware attacks. However brands like Quick Heal and Norton have a sizeable percentage of its user who is not happy with this feature of their Anti-virus software.

18. It is observed that all the brands of Anti-virus software provide ’manual scanning’ facility in addition to ‘auto-scanning’ facility. This feature, although redundant is provided for the satisfaction of users. Who can manually scan specific storage devices and be assured that they have scanned a particular area or device. This is not possible in case of auto-scanning which takes place in the background. Majority of the user are happy with this facility provided by their Anti-virus software provider.

19. It is revealed in the course of the study that ‘Compressed File scanning’ capability of all the brands does not provide the protection of virus attacks that sometimes enter the system through compressed files and folder thus this feature is not up to the satisfaction of the different users.

20. The study reveals that ‘Virus Protected File Sharing’ capability of all the brands does not provide for protection from virus that may enter the system through the network. When a machine is connected through a network and as a part of network the machine shares files from other machines in the network. This file if infected carries malware into the system. Thus, this feature of scanning shared files is not up to the satisfaction of the different users.

21. It is revealed in the course of study that majority of the users are not satisfied with the ‘email scanning’ capability of all brands of Anti-virus software. Because this facility fails to give complete protection from viruses that may enter the system through ‘Push-Up’ and ‘Pop-Up’ mails. Thus this feature is not up to the satisfaction of the different category of users.

22. It is observed that the internet offers a plethora of online facilities in the form of web based applications. And a desktop computer can not be isolated from the web. These applications (facilities) are available free of cost. Therefore the cost of development and maintaining is recovered through advertisements which are placed on the web pages of this application. These advertisements are dynamic and appear as pop-up. And the term used for such advertisements is ‘adware’. Such adware that finds its way into any machine accessing the internet may carry a malware. Hence the adware scanning capability is incorporates in all Anti-virus
software. However it is revealed that this capability of all the brands fails to give complete protection from viruses that may enter the system through ‘Push-Up’ and ‘Pop-Up’ mails. Thus this feature is not up to the satisfaction of the different category of users.

23. This study has revealed that all the brands of Anti-virus software have an inbuilt capability of ‘script blocking’. Script languages are frequently used to execute malicious code from web sites. Many Anti-virus programs have the ability to monitor Java, ActiveX, Visual Basic and other script files and detect and block malicious activity. However all the brands of Anti-virus software studied, fail to stop micro-virus from entering the system through various scripts. Thus this feature is not up to the satisfaction of the different category of users.

24. The study reveals that ‘Heuristic Scanning’ is basically used to evaluate unknown and suspicious objects by simulating the object's behavior in a safe virtual computer environment. The behavior is then analyzed, and it is decided if the object can be dangerous to the computer or not. This allows detection of malicious code not yet described in the virus database. The Heuristic scanning capability of any Anti-virus available off-the-shelf is not up to the expectation of the users.

25. The study reveals that scanning of ‘Quarantined Infected Files’ is found to be unsatisfactory. Majority of the users are not satisfied with facility provided by the Anti-virus software provider. Quarantining of any file with suspected malware is a simple process whereas scanning of these files while in use is a complicated process that would reduce the speed of the system. Hence, this facility is not incorporated so as to maintain the speed of computer machine.

26. The study reveals that many worms and other malware can now be spread through instant messaging programs. To stop this, Anti-virus software developers provide the facility of ‘instant message scanning’. However, this facility provided by all the brands most of the time fails to stop intrusion of malware through the instant messages received by the system. Thus this feature is not up to the satisfaction of the different category of users.

27. The study reveals that the ‘registry start-up’ facility provided by all the brands is not up to the expectation of the users. Majority of the users are not satisfied with this facility provided by their Anti-virus software provider.
28. The study reveals that majority of the users are not satisfied with the ‘Web-Mail Scanning’ facility provided by their Anti-virus software provider. Web Mail Scanning is the ability of Anti-virus software to scan the attachments of mail that are received by the system. This feature with all the brands of Anti-virus software is not up to the satisfaction of the different category of users.

29. It is observed that that the ‘Online Support’ service provided by all the brands is below the expectations of the users. Since most of the times the users when in need of on-line trouble shooting take the option of messenger service provided however most of the times this service is not available due to busy server of the service provider and hence the user has to revert back to email service which is not instant thus the users have to wait for the reply (solution) which may take more than 24 hours.

30. It is found that the ‘Telephonic Support’ service provided by all the brands fails to satisfy the users. Since most of the times the users when in need of solution to their problems related to viral infection or installation process of the Anti-virus software, take the option of telephonic support service. However most of the times this service is not available due to busy telephone lines.

31. It is found that the ‘Technical Support’ service provided by all the brands is prompt and up to date. Majority of the users are satisfied with this service provided by their Anti-virus software provider.

32. The study reveals that that the ‘User Manual’ provided by all the brands is easy to understand and follow with the illustrative snapshots and graphics provided. Majority of the users are satisfied with this service provided by their Anti-virus software provider.

33. The study reveals that the ‘User Forum’ facility provided by all the brands is generally useful to the users. Majority of the users are satisfied with this facility provided by their Anti-virus software provider. User forum helps to share ideas related to the Anti-virus software installation and virus protection from other users through posting of blogs on the forum. In this manner solutions can be obtained to different problems related to virus protection and data security. However it may also be noted that a sizeable percentage of the users are not satisfied by this facility in case of some of the brands like Quick Heal, McAfee and Norton.
34. It is observed that ‘On-scan reporting’ provided by different Anti-virus software a provider is up to the satisfaction of the users. On-scan reporting is usually in a tabular form, which displays the total number of files scanned, total number of files repaired, total number of files deleted, total number of files quarantined, details of infected files, level of malware and description of malware. Majority of the users are satisfied with this facility provided by their Anti-virus software provider.

35. The study reveals that the ‘Password Protect’ setting service provided by all the brands is not being used by most of the users and hence they are not aware of this feature.

6.3 CONCLUSION;

It is concluded that there are six popular brands of Anti-virus software being used by the different categories of users in the districts of Sangli and Kolhapur. It is revealed that each of the brands of Anti-virus software offer different variants of their solutions to suit the differing needs of the different users. The various factors that influence the users’ decision to buy a particular brand of Anti-virus software were also revealed and the investment made by the users in Anti-virus software was also found. The study, on the basis of the key performance indicators, which were used as parameters that were ranked by the users, reveals the performance of the various brands of Anti-virus software in the market and on the basis of which the various brands have been ranked.

B) SUGGESTIONS:

B: 6.1 Introductions:

In this part of thesis the researcher has proposed some suggestions based on the observations and findings presented in the previous section and also on the basis of the interaction the researcher has had with the users and discussed the various issues related to the anti virus software in use. It is divided into 3 sections.

Section – I contains suggestion that are common to the entire user category and all brands of Anti-virus software.

Section – II comprises of suggestion and recommendations to the Anti-virus software developers on brands enhancement of the performance of their Anti-virus software.
this section the researcher has made suggestion related to the key performance indicator whenever necessary.

Section – III is devoted to the benchmarking model developed by the researcher as a suggested model for benchmark of Anti-virus software.

**B: 6.2 Section I – Common suggestion to the entire user category and all brands of Anti-virus software.**

The study would like to make certain suggestions to all the users belonging to the different categories.

1. It is suggested that, all the users should install a licensed copy of Anti-virus software. Pirated or trial versions of Anti-virus software do not fully protect the system, because several functions are not made available in a trial or pirated copy of Anti-virus software. The study would like to mention that saving on cost towards an Anti-virus software would be unwise because in the short term trial versions and pirated versions may serve the purpose of protecting the system but in the long run such copies of Anti-virus software will fail miserably resulting in loss of data, intrusion of spyware that would result in unsecured transactions and considerably reduced speed of the machine.

2. Based on the observations made during the study it is suggested to all the users of Anti-virus software that they should enable all the functions and capabilities of the software. Especially, the default settings it is observed that almost all the users except for banks disable some of the function or capabilities provided by the developers which seemingly are of no much use. However, these functions when disabled may render the system ‘unprotected’ from malicious code at a later period of time. Therefore it is advisable to take the services of an expert or a consultant or the developer’s installation instructions while installing the Anti-virus software because the Anti-virus software of today may be small in size but are slightly complex in their function and thus require expert advice during installation.

3. The study would like to suggest to the users that popular brand name does not necessary mean reliable or dependent. Therefore the user is advice to visit the website of the different brands and make a comparative study of the facilities and capabilities provided by the Anti-virus software before comparing the price and
support service. It is also advisable to see the number of years the Anti-virus software developers is in the business and the technology being used by them, because these features are responsible for building a reliable Anti-virus software application to a certain extent.

4. Based on the findings and observations, it is suggested that all the users, regardless of the nature of work done on their computer system should use the ‘total security’ type of Anti-virus software because this type of Anti-virus software provides all round security by protecting the machine from intrusion of most of malware. This is not possible in case of ‘Home edition’ type of Anti-virus software which provide only basic protection to the computer system.

5. Based on the findings of the study it is suggested that to derive maximum benefits from Anti-virus software, it is advisable to read and understand the online help document provided by the developer before and after the installation of the software. This will help in configuring the Anti-virus software to the exact needs of the users on one hand and on the other it would protect the system from the latest malware which are in circulation.

B: 6.2 Section – II - Suggestion and recommendations to the Anti-virus software developers on brands enhancement of the performance of their Anti-virus software

1. Although the ‘virus definition update’ facility provided by all the brands of Anti-virus software are satisfactory it is suggested that latest search engine technology may be used to protect the system from latest malware without consuming much time.

2. The success of Anti-virus software largely depends on ‘virus definition update’ and ‘version update’. Version update is necessitated due to technological upgrade or functional update. These updates today have become an ongoing process since new malware keep appearing on the scene very often. Hence it is advised that all the brands should be proactive in their approach towards version update, which is possible through a strong research and development.

3. Secondary storage devices like pen drives, flash drives, memory cards, external devices that are attached to a computer system are the chief carriers of malware. Therefore, it is suggested to all users to scan such removable disks before
accessing any files or folder from such media. All the Anti-virus software have this provision of ‘on-access scanning’ of secondary storage devices and repairing or quarantining infected files. However, this on-access scanning process differs from brands to brands. It is suggested that on-access scanning should be done in the background and quickly. And if the infected file is accessed, then the file should be scanned, repaired, and made available instantly. The progress of such scanning may be displayed in the task bar. In the case of secondary storage devices like CD, DVD, MP3 etc. which are recordable media on-access scanning by Anti-virus software can only display an alert of infected file but cannot repair or delete or quarantine files. In such cases best alternative would be to copy the files and then scan and repair the files, provided the malware is identified by the Anti-virus software on the machine.

4. It is suggested that the ‘on-demand’ scanning capability provide by all the Anti-virus software developers should display the scanning process more vividly using better graphics so as to assure the user that the storage devices has been thoroughly scanned for the various malware and what corrective measure has been taken. This graphic illustration should be followed by a report of the details.

5. During the course of study it is observed that scheduled scanning facility provided in the Anti-virus software is used by majority of users. Scheduled scanning is a provision to schedule an entire system scanning on a given day of week and time. The Anti-virus software will scan the machine on the specific day and time automatically provided the machine is switched on at that specific day and time. If in case the machine is switch off at that specific time then scheduled scan lapses and later when the machine is switched on there is no way the user can come to know about the lapse in scheduled scan since there is no alert message displayed. Hence it is suggested that if in case there is lapse in the scheduled scanning due to the machine not being in use at the specific time then the Anti-virus software should have a provision to alert the user about the lapse in scheduled scanning when the machine is switched on after the lapse.

6. Auto clean infected file scanning facility is a process when the Anti-virus software scans the quarantined infected files or infected files in the chest. This process, which runs in the background, gives alert message to the user as to which are the files that need to be cleaned? Therefore it is suggested that the user
physically delete all the infected files in the chest or those quarantined and get rid off the messages.

7. It is suggested that manual scanning features should have illustrative graphics to display the scanning process disk by disk followed by a report on details of files scanned, files infected, name of malware etc. this would satisfy the user and assure him that his machine is clean.

8. In case of compressed files that are received by the system can not be scanned by Anti-virus software. Thus there is every likelihood of intrusion of malware through compressed files. Therefore it is suggested that the Anti-virus software developers in collaboration with file scanning software developers to understand file compressing and locking technology so as to enable their Anti-virus software to unlock and extract a compressed file and scanning for malware.

9. The rapid development in the field of networking, has enabled large number of computers systems to be connected with each other. These networked machines share large amount of data which are transferred from one machine to another machine in the form of data files. Such files cannot be scanned for viruses. The only way out is to map all the machines on the network and scan each storage device. This is practically not possible when number of machines is large. Therefore it is suggested that the Anti-virus software developers should develop a technology to scan viruses in the network that find their way into the computer systems through shared files.

10. ‘Email scanning’ and ‘adware scanning’ is not possible by the existing Anti-virus software to the fullest satisfaction of the users since malware can enter into a system through ‘pop-up’ and ‘push-up’ mails through the Internet. A suitable and effective technology needs to be developed to scan such files. Presently the operating system or Anti-virus software display warning messages saying that the system is now connected to an unsafe source. Therefore it is suggested that the web server (source) from where the email and accompanying adware emanates should be requested (by the Anti-virus software) to certify that the transaction with this source is safe and the files are scanned for malware.

11. Most of Anti-virus software programs have the ability to monitor Java, ActiveX, Visual Basic and other script files and delete and block malicious code. However most brands of Anti-virus software fail to detect unidentified malicious code.
Therefore it is suggested that Anti-virus software developers should pay special attention to such script. Whose number is not large and scan them thoroughly for malicious code. Instead of the present practice of displaying alert messages, saying that such scripts may carry malware.

12. Heuristic scanning capabilities need to be improved by all the brands of Anti-virus software. It is suggested to properly analyze the behavior of suspicious objects and alert the user if that objects (files) could be dangerous to the system.

13. This study would like suggest to all Anti-virus software developers to upgrade the functions of ‘Registry start-up scanning’ because all the Anti-virus software fail to scan the registry keys at start-up. This may require technological upgrading.

14. It is suggested that the web server of all the Anti-virus software providing online support should upgrade their web server in terms of storage capacity and processing speeds to accommodate more and more online requests from their users for online trouble shooting tips or solutions.

15. This study would also like to suggest to all that brands of Anti-virus software developers to update their telephonic support services so as to accommodated maximum number of calls from their clients for solutions to their problems related to software installation or treatment of infected files.

16. The study would like specially recommend the Anti-virus software developers to make a special mention in the user manual or online help, to the users not to disable certain default settings and functions that may not be of use to the users at present but may be of great use in long run.

17. It is suggested that all the Anti-virus software developers should encourage its user to post blogs on the users’ forum as regards their observations or problems related to the various functions of their Anti-virus software. This can be a rich source of feedback for Anti-virus software developers that would help them to upgrade the software application.
B: 6.3 Section - III - The Benchmarking Model for an Ideal Anti-virus Software
The Researcher has suggested a model for ideal Anti-virus software, based on findings from the research study. Basically, in any Anti-virus software, the scanning process should start with accepting data for virus scanning. At this step, user must be given an interface to select the data for scanning. This selected data will be termed as ‘Incoming Data’ from this step onwards, by the Anti-virus software.

Now, after accepting data for scanning, at first instance, the software will check whether there are any unknown programs submitted for virus scanning. If Any, Then Anti-virus software will check, whether there are any Operating System filters components/files submitted as a part of incoming data. If there is no such unknown program found, then the control of scanning process will move to the next step, i.e. Deliver data.

If any operating system filter found, then the researcher suggests to have a provision for specific scanning of such components of operating system. As operating system is an interface between user and computer, there is a need of specific virus scanning of such data items. In absence of such operating system components, the data will be sent to the next step of scanning process.

At the next instance, there is need for checking whether status of Anti-virus software is ‘disable’ or ‘enable’. If disable, then there should be a provision for making it ‘enable’. If it is in ‘enable’ state, then virus scanning process will start.

As a part of virus scanning process, each data component submitted for virus scanning, will be scanned to check whether it is infected by any kind of virus attack, such as malware, Trojan, adware, spyware, boat, etc. Each Anti-virus package contains its own virus definition, which must be updated regularly.

Normally there are two outcomes of virus scanning process, ‘virus found’ and ‘virus not found’. In case of ‘virus not found’, then it will display the scanning process summary along with a message of ‘No virus found’. Hereby the scanning process will be terminated.

And, in case of ‘virus found’, next step in the scanning process is ‘disassembling’. In disassembling process, all infected files will be classified into three categories, a) files infected with virus, b) Encrypted data, in which no virus in scanable data c) completely unscanned data. For infected files, it will check whether the file is repairable or not. If yes, then perform action under repaired data handling and display the scanning process summary and process will be terminated. If infected
files are not repairable, then Anti-virus software should ask the user to quarantine or delete the infected file. Based on the user response, perform quarantine or delete action on infected files, display process summary and process will be terminated. If user does select ‘quarantine’ or ‘delete’ option, then Anti-virus software will perform action under infected data handling, display process summary and process will terminate. For encrypted data, in which no virus found in scanable data, perform action under encrypted data handling, display process summary and process will terminate. For ‘Unscanned data’, perform action under unscannable data handling, display process summary and process will be terminated.

6.4 – Performance Evaluation Software for Anti-virus Software [PESAS]

Figure 6.4.1 – PESAS Menu
CHAPTER VI

FINDINGS AND SUGGESTIONS

Figure 6.4.2 – User Basic Information

Figure 6.4.3 – Use Entry form for Anti-virus Performance Evaluation
Figure 6.4.4 – Use of Anti-virus Software

Figure 6.4.5 – District wise use of Anti-virus Software
CHAPTER VI  

FINDINGS AND SUGGESTIONS

Figure 6.4.6 – Use of Licensed or Trial Anti-virus Software

Figure 6.4.7 – District wise Performance of Anti-virus Performance
Figure 6.4.8 – Over all Performance of Anti-virus Performance

Figure 6.4.9 – District wise Priority for Purchasing Different Anti-virus Software
Figure 6.4.10 – Priority for Purchasing Different Anti-virus Software

Figure 6.4.11 – About Us
USER GUIDE

About PESAS

Performance evaluation software for Anti-virus software [PESAS] is tool designed to evaluate performance of Anti-virus based on various performance indicators. With very few input this software will give you the detailed performance report of each Anti-virus for different type of users.

Minimum System Requirements

Windows

- Windows 98, Windows 2000, Windows XP, or Windows 7
- Pentium II, 200 MHz or greater
- 64 MB RAM (128 MB is recommended, and required for Windows XP)
- Mouse
- 1024 x 768 screen resolution
- CD drive / USB Drive
- 200 MB hard disk space

Macintosh

- Mac OS 10.1
- 128 MB RAM
- Mouse
- 1024 x 768 screen resolution
- CD drive / USB Drive
- 250 MB hard disk space

Installation

Before you install PESAS, you must close all other applications, including virus detection programs. If other applications are running, they may interfere with the normal installation process. In Windows, open applications are displayed on the taskbar.

PESAS has a simple installation procedure. Double click on PESAS setup file. During installation, read each installation screen, follow the instructions, and then click ‘Next’ to continue. After successful installation restart the computer. PESAS has no need to be registered upon installation.
Using PESAS

PESAS can be accessed from the desktop as follow
By clicking Start -> Programs -> PESAS Tool -> PESAS.

PESAS Menus

PESAS menus give you instant access to menus, reports and about us topics. PESAS menus are at the left side of the main window and are always available irrespective of the feature being accessed. PESAS menus are as follows:

1. **Anti-virus user information**
   - This is the first menu of PESAS, this menu enables you to fill the information. On click of this menu user information screen will display. Which has five different tabs, user has to fill up all the required information about their Anti-virus?

2. **Anti-virus Performance Evaluation**
   - On click of this menu Anti-virus performance evaluation screen will display. Through this menu you can check the performance of different Anti-virus used by various users.

PESAS Reports

PESAS reports give you instant access to all the reports. PESAS broadly categorize in to two categories Anti-virus software’s used by different users and performance evaluation reports.

6.5 - SCOPE FOR FUTURE RESEARCH

Anti-virus products will be on the scene until viruses/malware are there to attack computer systems. Therefore this area of computer system security and protection provides ample scope for further research studies. Some of the aspects of Anti-virus software that can be investigated are as follows:

- Development of metrics that are objective and can be replicated and reproduced by third parties for measurement of performance specific to the following:
  - Desktop Protection for all operating systems
b) Web Browser & E-mail Protection  
c) Internet Gateway Protection  
d) Network Server Protection  
e) Real-Time Boot Virus Protection  

- Devise a mechanism to measure the capability of Anti-virus software to protect all points of entry into a system.  
- Study and evaluate the technology applied by the different players in the Anti-virus software market.  
- Devise a method to show the levels of protection of an enterprise (Viz. Latest/Recent/Old/Obsolete viruses defined).

6.6 CONCLUSION:  
The study, on the basis of the findings has made some suggestions firstly to all the categories of users that are general in nature as to what are the key parameters that one should look for to get the best protection from virus and other malware. Secondly suggestions and recommendations are also made to the Anti-virus software developers as to the enhancement of the performance of their software solutions on the basis of the key parameters. Lastly the study has developed a model for benchmarking the Anti-virus software so as to help the developers to provide a foolproof solution to deal with virus and other malicious codes and also to guide the users to find the Anti-virus software that best suits their individual needs. In the end the study has listed out the areas that can be taken up for future research in this field of Anti-virus software development.