CHAPTER 5
FINDINGS, SUGGESTIONS AND SCOPE FOR FURTHER RESEARCH
CHAPTER 5
FINDINGS, SUGGESTIONS AND
SCOPE FOR FURTHER RESEARCH

5.0. INTRODUCTION:

This chapter is aimed at presenting the important findings from the study. Subsequently, the conclusion drawn from the study and suggestions arising out of the study have been presented.

During the course of study and secondary data, in particular, it was found the previously published research material on this particular area of the study was very limited. A number of areas and aspects required wider and in-depth research. The scope for further research is, therefore, briefly discussed before concluding the chapter. For ready reference and convenience, table numbers of the study are given in brackets in the concerned paragraph of the chapter.

5.1. FINDINGS:

In this section, findings which were made in the previous chapters have been recapitulation in a short form. Four objectives and three hypotheses have been used for carrying an in-depth study on the subject. The fifth objective is part of suggestions as it aims to provide a theoretical model as solution for correcting some of the problems found in the ICT facilities as outcome of the study.

The researcher has analyzed the primary data to study the current status of implementation of I.C.T. infrastructure facilities and services and its security in Higher Technical Education institutions in Pune region. The researcher has done the assessment on the subject by collecting data and analyzing it according to 4 respondent types namely I.C.T. support Staff, Full-Time Teaching Staff, Full-Time Students, and Heads of Institution.
Therefore, in this section we provide the summarized findings from these 4 respondents in Four parts viz. Part I: Findings from I.C.T. Technical Staff, Part II: Findings from Full-Time Teaching Staff, and Part III: Findings from Full-Time Students, and Findings from Heads of Institutions.

5.1.1 PART I: FINDINGS FROM I.C.T. TECHNICAL STAFF:

I.C.T. Technical Staff is the actual person who is responsible for setting-up the I.C.T. infrastructure, maintaining it and upgrading it from time to time as per requirements. It is also their responsibility to secure the I.C.T. infrastructure from physical damages as well as security compromises.

Data from I.C.T. technical Staff was analyzed on following points Total PCs, Norms followed for creating I.C.T. infrastructure, I.C.T. implementation support source, Number of I.C.T. Technical Staff employed in the institution, Availability Laptops, printers, etc. available to students and staff for use, Type of PCs and Servers used (Branded/ Unbranded), Software Type used the institution (Open-source, licensed, etc.), Speed of internet Connection, Type of Internet Connection, Purpose of using institution’s I.C.T. infrastructure, ERNET services used by institution, Availability of Wi-Fi, Audit frequency, Maintenance of Internet usage logs, Drafted ICY policy in the institution and its display in the institution, Extent of satisfaction w.r.t. to I.C.T. services by the institution, Measures to improve user satisfaction Extent of satisfaction w.r.t overall I.C.T. infrastructure security, Extent of satisfaction w.r.t. overall I.C.T. Digital assets security, Level of I.C.T. security attacks encountered. Role in preparing I.C.T. Policy, Licensed Antivirus software available of PCs and Servers, Factors influencing increase in I.C.T. security attacks / lapses, Factors which help reduce / prevent I.C.T. security lapse or attack, Areas that need to be addressed to reduce / prevent I.C.T. security lapse or attack, Percentage of Annual Budget is set aside for I.C.T. and Actual expenditure Percentage made on New purchases / Up-gradation of I.C.T., & Areas providing benefits and maximum Return of Investments on I.C.T..

- All (100%) of the engineering institutions having various range of student intake have the required or more number of PCs. Pharmacy institutions also showcase similar trends. Management institutes also depict a similar trend except for institutes having More than 900 but less than 1200 enrolled students where only 16.7% institutes have required or more amount of PCs. (Ref. Table 4.2). The
Management colleges which have higher number of enrolled students i.e. more than 900 but less than 1200, in majority of cases have lesser number of PCs than required by AICTE. Looking at PC-to –Student ratio where the minimum ratio is not obtained in middle sized institutions means such institutions are defying even A.I.C.T.E. and DTE Norms.

- 85.6% institutions have used Vendor Support to setupI.C.T. infrastructure facilities while 42.3% have used Internal Staff resources to do so. Only 32.4% have used services of Independent specialist consultants. **Low use of Specialist services shows that educational institutions have still not been able to match or adopt the industry culture and specifications w.r.t. I.C.T. implementation and its security. (Ref Table 4.3).**

- 82.9% Technical Staff have stated that their institution’s I.C.T. infrastructure facilities were created using A.I.C.T.E. Norms, DTE Norms was at 64.9%. Only 18% said they followed UGC norms (Refer Table 4.5). **This may be because UGC norms doesn’t directly apply to individual colleges but on Universities. As Management and Engineering are reporting to AICTE and DTE as regulatory body, this might be the reason they are following AICTE and DTE norms more.**

- As per Technical Staff Respondent’s views (Refer Table 4.7), PCs have been Ranked at No. 1 followed by Printers (Rank 2), Laptops (Rank 3), Scanners (Rank 4). This implies that according to Technical Staff, the institutions where they are serving PCs are most available for users. Deeper analysis shows that Technical Staff point out that PCs are 100% Frequently available along with Printers which are 77.48% frequently available. In contract, Laptops are 62.16% Never available and Scanners are 85.59% Never available. **In institutions PCs are available for use of students and staff frequently. Though Printers, laptops and Scanners might be available in the institute but students are not allowed to use them.**

- Only 3.6% Technical Staff respondents have opined that institute is using Non-Branded PCs and Servers. 49.5% respondents opined that their institution is using Branded PCs and Servers. These are good indications. **But 46.8% say**
that their institution is using a mix of Branded and Non-Branded Servers and PCs. (Ref Table 4.10). It is not clear regarding what is the proportion of Branded PCs and Servers in this. It must be understood that if percentage of Non-branded ones is more then it means that there is lot of compromise with security and safety of data as failure rate of non-branded machines is always a big question.

As per responses of Technical Staff w.r.t what type of software are used in their institute, Licensed Software have been Ranked at No. 1 (most frequently available and used) followed by Open-Source Software (Rank 2), Trial-version / Unlicensed Software (Rank 3), In-house developed software (Rank 4) by Technical Staff. Ignoring Neutral / Can’t Say responses, 88.20% technical Staff say that Licensed Software are Frequently used. This is followed by Open-source software (71.17%) and Trial-version software (56.76%). In contract to this 70.27% respondents say that In-house developed software are Never used in their institution. (Ref Table 4.12). This implies that according to Technical Staff, the institutions where they are serving, most of the software being used are licensed versions. Open-Source software which do not need any type of licensing are also much in use. Also Institutions like engineering and Management (MCA) are not using the talent and skills of their staff and students to develop software in-house.

As per Technical Staff’s responses 10 Mbps to 15 Mbps (45%) was the Internet Speed (bandwidth) that most Institutions were using whereas 15 Mbps and above (4.5%) was least been used. (Ref Table 4.16). All institutions have appropriate amount of Internet Bandwidth.

Broadband (51.35%) and Leasedline (48.65%) internet connections are most in use. Various factors for this include ease of installation and use, pricing, etc. (Ref Table 4.17). All institutions have some type of commonly used internet connection.

As per Technical Staff Respondent’s views (Refer Table 4.18) w.r.t purpose of use of ICT infrastructure facilities provided in the higher technical education institutes, Emails have been Ranked at No. 1 followed by Lecture Preparation
(Rank 2), and View Online lectures (Rank 3). This implies that most of the technical staff themselves mostly use their institutions I.C.T. infrastructure for Email. Job Searching (Rank 12) at last which means users do not search for Jobs using their institutions I.C.T. infrastructure. 99.1% Technical Staff respondents say that Email is frequently used which is followed by Lecture Preparation (86.5%). In contrast to this, 61.3% respondents say that Listening to songs and Videos and Job searching (49.5%) is not done by the users using the institution’s I.C.T. infrastructure. Users of I.C.T. use I.C.T. infrastructure of institution for Lecture Preparation and Viewing Online structure and they don’t use it for recreation / entertainment work like Listening to Songs and Videos or for Job Searching.

- As the Table 4.22 depicts, 18% of Technical Staff respondents say that their institution is connected to ERNET while 48.6% respondents say that their institution is not connected to ERNET. Majority of institutions are Not Connected with ERNET (48.6%).

- 86.49% I.C.T. Technical staff respondents say that their institution has Wi-Fi network installed while only 13.51% respondents say that their institution doesn’t have Wi-Fi network installed. (Ref Table 4.23). Majority of institutions have Wi-Fi network. This is good indication but it is not clear whether Wi-Fi internet availability is allowed for students or it is just limited to usage by Staff and Management.

- As per Technical Staff Respondent’s views w.r.t. Satisfaction with certain I.C.T. services (Refer Table 4.24), Internet services through wired network has Ranked at No. 1 followed by Maintenance / Technical support (Rank 2), and Communication facilities (email, SMS, alert messaging, etc.) (Rank 3) and show weighted averages that correspond to Satisfied. Administration software, Storage and Backup utilities Rank at 7th and 8th. Of these, Storage and Backup Utilities show weighted averages corresponding to Neutral. Further analysis shows that in case of Storage and Backup utilities the number of respondents who are satisfied (44.14%) far exceeds the number of respondents that are dissatisfied (23.42%). This implies that respondents are actually satisfied with it. Thus, there are no
I.C.T. services or facilities offered by institutions with whom users are not satisfied as per Technical Staff.

- As per responses of Technical Staff w.r.t. measures for improving user satisfaction, *Increase in number of technical support staff* (87.4%) is the most required measure whereas *Provide after-hour lab facility* (18%) is one of the least required measure for satisfaction enhancement as per Technical Staff. (Ref Table 4.28). **Technical Staff has greatly emphasized on training of technical staff and also increasing their numbers in the institutions. They have also asked for replacing old PCs and Servers.**

- Weighted averages from Technical Staff responses suggest that these respondents are *Satisfied* (4.01) overall I.C.T. infrastructure security. In fact 91.89% of Technical Staff respondents have shown positive response. (Ref Table 4.30). **Majority of Technical Staff are Satisfied overall I.C.T. infrastructure security.**

- Weighted averages from Technical Staff responses (3.76) suggest that these respondents are Satisfied with overall I.C.T. digital assets security provided by their institution. In fact 79.3% of Technical Staff respondents have shown positive response. (Table Ref- 4.32). **Majority of the Respondents are Satisfied with overall I.C.T. digital assets security provided by their institution.**

- The highest weighted Average is for Low intensity attacks (3.8) followed by Mild (2.43) and (1.88). In case of low intensity attacks the highest frequency of occurrence is at 4 with a response (43.2%). In case of Mild intensity attacks the highest frequency is at 2 with a response frequency (38.7%). In case of High intensity attacks the highest frequency is at 1 with a response frequency (47.7%) (Ref Table 4.34). **This means that though mild and high attacks are also occurring but it is the Low Intensity attacks, which even though might not do lot of destruction or losses, but are most frequently occurring out of the three and their occurrence is nearly moderately high.**
• As per Technical Staff’s responses, we find that majority of these respondent’s role in Policy Making is confined to Consultative (82.9%) (Ref- Table 4.40). This means that Technical Staff mostly give consultation but they are not the final decision makers even though they have best technical and operational knowledge in this area.

• 33.3% Technical Staff state that their institute doesn’t have a formal I.C.T. Upgradation policy while only 18.0% say it is present (Ref Table-4.41). Majority Technical Staff says their institute doesn’t have a formal I.C.T. upgradation policy.

• As is evident from the Table 4.43, Technical Staff (53.2%) state that All Servers have antivirus installed on them whereas 43.2% state that Few Servers have antivirus installed on them. This means that majority respondents state in their institution all servers are protected by antivirus but considerable number them also state that in their institutions antivirus is installed only on few servers.

• Table 4.43 states that 30.6% Technical Staff state that All PCs have antivirus installed on them whereas 69.4% state that Few PCs have antivirus installed on them. This means that in majority institutions All PCs used by students and staff members are not protected and this is a great danger to the security of the data.

• The factors namely Lack of Technical staff(4.43), Carelessness of users(4.38), Lack of equipment / technology / software in the institution to avoid I.C.T. attacks Ranked I, II and III and showed weighted average corresponding to High Role. Lack of hardware / data ,etc. disposal policy, Lack of Content management, Lack of Data Governance (Management/storage/dispersion) policy, and Lack of fixation of responsibility and liabilities on users which are ranked at 14th, 15th, 16th and 17th rank show weighted averages which correspond to neutral responses from Technical Staff respondents. Further analysis of these factors reveal that in case of Lack of Technical staff (92.8%), Carelessness of users (83.8%), Lack of equipment / technology / software in the institution to avoid I.C.T. attacks (88.2), Lack of hardware / data, disposal policy (9.55%), Lack of
Content management (28.83%), Lack of Data Governance (Management/storage/dispersion) policy (40.54%), and Lack of fixation of responsibility and liabilities on users (41.44%) Technical Respondents have stated that these factors have a High Role in committing of I.C.T. Security attacks. (Ref Table 4.45). Top most factor which play major role in committing of I.C.T. security attacks include Lack of Technical staff, Carelessness of users, Lack of equipment / technology / software in the institution to avoid I.C.T. attacks. Lack of Content management, Lack of Data Governance (Management/storage/dispersion) policy, and Lack of fixation of responsibility and liabilities on users are at the bottom of the list.

- (Ref-Table 4.46) As per Technical Staff responses, Antivirus, firewall, auto-updates, etc. (4.5; 90.99% high role responses) Ranks at No. 1, and comes under the category of Very High role in reducing / preventing I.C.T. security attacks. This is followed by Technical staff able to manage I.C.T. infrastructure and its security (4.26; 78.38% high role responses; ) and Educating of staff and students about I.C.T. laws and Best Practices (3.77; 67.57% high role responses) which come in the category of High Role. Security audit able to find gaps in I.C.T. security (2.66; 13.51% high role responses; 39.64% low role responses) shows that it falls in Average Role category and finds its place at the end of the list. Antivirus, firewall, auto-updates, etc, Technical staff able to manage I.C.T. infrastructure and its security, and Educating of staff and students about I.C.T. laws and Best Practices are the top ranked factors which play major role in reducing / preventing I.C.T. security lapse or attack as per Technical Staff.

- As per Technical Staff, Stringent Penalties (74.8%) is the most important Areas that need to be addressed to improve I.C.T. security in the institutes. This is followed by Identification and blocking loopholes in security (73.0%) and User Awareness about cyber laws (72.0%). Changes in routines, beliefs and informal norms used in the organization (44.1%) is the least important area. (Ref Table 4.49). Technical staff’s solution for improvement in I.C.T. security are mainly aimed at users and include penalties as well as user education.
• Technical Staff have given highest responses (30.6%) to 15% to 20% of annual budget is set aside for I.C.T. (Ref- Table 4.52). But on an average only 16.7% of Annual Budget is set aside for I.C.T. (Ref- Table 4.53) as per Technical Staff. The percentage of annual budget set aside for I.C.T. is quite low as compared to recurring and non-recurring annual costs related to I.C.T. Very little is left for up-grading hardware and for purchasing new licensed software. The avg. I.C.T. budget is only 16.7% of total annual budget.

• As per Technical Staff, the highest responses have been received by (ignoring Can’t say responses) 40% to 60% of sanctioned I.C.T. budget actually utilized (27.9%). (Ref Table 4.54) On an average 50.28% of the budget set aside for I.C.T. is actually used. The actual spending on I.C.T. is very low as compared to what has been set aside in the annual budget.

• 83.8% Technical Staff have said that they agree that “Investment in I.C.T. is Every penny Worth”. (Ref- Table 4.56). Majority of technical staff understand that investment in I.C.T. infrastructure is good for the educational institution.

• As per Technical Staff Respondent’s views (Refer Table 4.58), Communication (4.18) with 90.09% positive responses has Ranked at No. 1 followed by Stationary (e.g. paperless office) (Rank 2, 4.07) with 76.58% positive responses, and Information storage and access (Rank 3, 4.05) and show weighted averages that correspond to High Returns on Investment.

Areas like Manpower (Teaching, Non-teaching, etc.) staff, Examination process, Decision making, Automation and integration, and Others depict weighted averages which point out towards Neutral responses. Ignoring Neutral responses, further analysis reveals that in case of Manpower (Teaching, Non-teaching, etc.) staff the responses for High return (42.34%) are more than those for Low (11.71%).

In case of Examination process, the responses for High return (52.25%) are more than those for Low returns (23.42%). In case of Decision making, the responses for High return (28.83%) are more than those for Low returns (11.71%). In case
of Automation and integration, the responses for High return (36.04%) are more than those for Low returns (14.41%). This indicates that technical Staff feels that there is positive benefit / Return from Investment in I.C.T.especially in the field of Communications and Savings on Stationary.

- As per Technical Staff Respondent’s views regarding Benefits Provided by I.C.T. (Ref Table 4.63), Increase in admissions (Avg. weight 4.47, 86.48% positive responses towards agreement) has Ranked at No. 1 and show weighted averages corresponding to Strongly Agree.

This is followed by Expand expertise base (Rank 2, Avg. weight 4.43, 87.39% positive responses towards agreement) and Standardize processes (Rank 3, Avg. weight 4.39, 96.39% positive responses towards agreement) and show weighted averages that correspond to Agree. Reduced payback period (Avg. weight-3.48) and Understand changing environment and requirements (Avg. weight 3.36) are benefits that have been Ranked 25th and 26th respectively and land at the bottom of the list. Ignoring Neutral/ Can’t say, further, analysis of these 2 benefits reveals that in case Reduced payback period the Agree responses (48.65%) are more than Disagree responses (19.82%). Similarly, in case of Understand changing environment and requirements, the Agree responses (49.55%) far exceeds Disagree responses (17.12%). Colleges have been using I.C.T. as a factor for Increase in admission. They want to attract students by showing that they have internet, Wi-Fi facility and computer labs. Standardization of day-to-day institutional processes is also an area which institutions are looking at using the help from I.C.T..

5.1.2 PART II: FINDINGS FROM FULL-TIME TEACHING STAFF:

Full-Time Teaching is one of the main end-users of I.C.T. infrastructure and facilities in institutions of Higher Technical Education. Today’s higher education systems is gradually moving from Blackboard to Electronic presentation skills. Thus, their opinion regarding various facets of I.C.T. infrastructure and services offered in institution of service is quite important.

For this type of respondent, primary data was collected using questionnaires from 332 respondents who were working as full-time paid teaching staff at Professional higher
technical education institution running A.I.C.T.E. approved course and teaching only A.I.C.T.E. approved course.

In this case the data collection collected and analyzed based on following points (excluding certain general institute-related information) viz. Total Number of Fulltime enrolled Students (including all years), Courses Conducted (A.I.C.T.E. Approved only), Total Number of Full-time Teaching Staff members, Total Number of PCs in the institution for the said course, Availability Laptops, printers, etc. available to students and staff for use, Type of PCs and Servers available in the institution, Software Type used the institution (Open-source, licensed, etc.), Norms followed for creating your I.C.T. infrastructure, Purpose of using institution’s I.C.T. infrastructure, Extent of satisfaction w.r.t. to I.C.T. services by the institution, Measures to prove improve user satisfaction., Extent of satisfaction w.r.t overall I.C.T. infrastructure security, Extent of satisfaction w.r.t. overall I.C.T. Digital assets security, Level of I.C.T. security attacks encountered, Success factors influencing reduction / prevention of I.C.T. security lapse, Areas to be addressed to improve I.C.T. security, Percentage of Annual Budget is set aside for I.C.T. and Actual expenditure Percentage made on New purchases / Up-gradation of I.C.T., Whether investment in I.C.T. infrastructure is every penny worth spent, Areas providing benefits and maximum Return of Investments on I.C.T.,

- As per Full-time Teaching Staff, A.I.C.T.E. Norms (71.7%) is most followed norm but DTE Norms (18.7%) are least followed. (Ref- Table 4.5).

- As per Full-Time Teaching staff (Ref-Table 4.8), PC (4.46) have ranked FIRST, followed by Printer (3.57), Scanner (2.75), and Laptop (2.69). Here, PCs score 95.20% positive responses for frequently used. But Scanner’s score for negative response for frequently used is 53.30% and Laptop’s negative response for frequently used is 59.90%. Teaching Staff have highlighted that though PCs are frequently available but Scanners and Laptops are not available to users (here Teaching Staff) for use.

- As per Full-Time Teaching Staff, (Ref- Table 4.10), most commonly used PCs and Servers are Branded (73.5%). Only 0.6% are non-branded. Teaching Staff have opined that most institutions are Branded.
As per Full-Time Teaching Staff, (Ref- Table 4.13) Licensed Software (4.54) are ranked FIRST with 96.69% positive responses for Frequent usage. Open-source software (3.11) are at SECOND rank with 49.70% positive responses for Frequent usage. Trial version software (2.89) are at THIRDrank with only 39.46% positive responses for Frequent usage. Teaching staff have opined that though licensed software are mostly used followed by open-source software but higher education institutions are under-utilizing their talent by not developing software in-house. Approx. 40% usage of Trial Version software is also quite worrying for the security point of view.

As per Full-Time Teaching Staff (Ref- Table 4.19), Research Work (4.46) is Ranked FIRST as most frequently used I.C.T. services with 91.87% positive responses for frequently used followed by Email (4.38) with 86.45% stating that they frequently use it. Job Searching and Listening to Songs and Videos are at bottom of the list with only 6.93% and 7.83% frequent used responses respectively for them. According to Teaching Staff, they use I.C.T. infrastructure for Research Work and Emailing mostly and refrain from using institution’s I.C.T. for personal work like Job Search and Listening to songs and videos.

As per Full-Time Teaching Staff views w.r.t. satisfaction with certain I.C.T. services and facilities (Refer Table 4.25), they are most Satisfied with Communication facilities (Rank FIRST) with 75.30% giving positive responses for Satisfaction. Internet services through wired network (Rank SECOND) has attained 91.87% positive responses for satisfaction. Maintenance/Technical support has attained THIRD rank with 84.04% positive responses for satisfaction. Ignoring neutral responses, we find that I.C.T. Security policies and Security facility & Storage and Backup utilities which are at the bottom of the list and have attained only 24.10% and 26.51% positive responses for satisfaction. But dissatisfaction for these two are only 3.25% and 2.92% respectively. According to Full-Time Teaching Staff, they are most satisfied with Communication facilities and Internet Services through Wired Network. Though Security policies and Security facility & Storage and Backup utilities
landed at the bottom of the list but still the majority of Teaching staff (ignoring neutral responses) have shown satisfaction with them.

- Full-Time Teaching staff have strongly opined that Antivirus (93.1%) if installed on PCs and Servers in the institution will really help in increasing user satisfaction among them. This is followed by ERP and other software used for teaching-learning (87.7%). The third important factor is Increase in number of technical support staff (83.4%). Replace old PCs, laptops, etc. (69.9%) is at the bottom of the list (Refer Table 4.28). **This means that Full-time Teaching Staff really feels the absence of Antivirus on PCs in the institute. They also feel that ERP usage will help in better administration and presence of other Teaching-learning software will help in improving teaching process. They also feel the absence of qualified I.C.T. technical staff in the institute as user’s PCs and network might not be repaired on time. They also feel that they should get representation in developing I.C.T. security policy and this updation should be done more frequently. Old PCs and Servers, etc. should also be replaced. As all these factors have got more that 50% YES responses so this means that this is the call of the majority of Teaching staff responses and, thus, can’t be ignored.**

- Full-time Teaching Staff w.r.t. overall I.C.T. infrastructure security are overall Satisfied (3.87) with 81.63% respondents showing positive responses towards satisfaction. (Ref- Table- 4.30).**Full-Time Teaching Staff is on a average satisfied with overall I.C.T. infrastructure security in their higher technical education institution.**

- Full-Time Teaching Staff w.r.t. overall I.C.T. Digital assets security are overall Satisfied (3.78) with 75.30% respondents showing positive responses towards satisfaction. (Ref- Table- 4.32).**Full-Time Teaching Staff is on a average satisfied with overall I.C.T. Digital assets security in their higher technical education institution.**

- As per Full-Time Teaching Staff, The most frequently occurring I.C.T. attacks are Low intensity attacks (1.91) followed by Mild (1.45) and (1.36). (Ref- Table 4.35) This means that **as per Full-Time Teaching Staff though Low, mild and**
high attacks are also occurring but their frequently occurring is very low. Of the three it is the Low intensity attacks which is most occurring and is occurring at moderately low rate. Mild and High intensity attacks are occurring but at Low occurrence rates as compared to Low Intensity ones.

- As per Full Teaching staff, 38.3% say that their institution doesn’t have I.C.T. up-gradation policy while only 23.5% say it is present (Ref- Table- 4.45). Ignoring Neutral responses, majority Full-Time Teaching Staff say that their institution doesn’t have a formal I.C.T. up-gradation policy.

- W.r.t factors which might play a major role in reducing / preventing I.C.T. security lapse or attack, as per Full-Time Teaching Staff responses, Technical staff able to manage I.C.T. infrastructure and its security (3.29; 50.6% High role responses) is ranked First, followed by Educating of staff and students about I.C.T. laws and Best Practices (3.27; 54.2% high role responses), and Physical security of campus / building like CCTV, biometric access controls (3.08; 35.8% high role responses) at the Second and Third Rank respectively. All these fall in the category of Average Role. Institution’s I.C.T. security policy is able to secure I.C.T. infrastructure and data assets (2.23; 11.4% high role responses) comes at the bottom of the list falls in the Low Role category. (Ref Table- 4.47). As per Full-Time Teaching Staff, Technical staff able to manage I.C.T. infrastructure, Educating of staff and students about I.C.T. laws and Best Practices, and Physical security of campus / building like CCTV, biometric access controls can play an average role in preventing I.C.T. attacks. They don’t have much faith in Institution’s I.C.T. security policy as an instrument to secure I.C.T. infrastructure and data assets.

- W.r.t. Areas to be addresses to improve I.C.T. security in the institutes, Full-Time Teaching Staff have given highestYes responses to User Awareness about cyber laws (YES: 87.65%) followed by Train users to identify I.C.T. security risks (YES : 86.4%). Stringent penalties (YES: 74.1%) is least preferred area.(Ref table 4.49) As per Full-Time Teaching Staff, most important areas to improve I.C.T. Security is User Awareness about Cyber Laws and Train users to identify I.C.T. security risks. They do advocate Stringent Penalties
(which might be for carelessness in carrying out duty by employees) but this is the last thing to do according to them.

- According to Teaching Staff, (ignoring Can’t say responses) 9.9% have stated that 5% to 10% of annual budget is set aside for I.C.T.. 7.5% respondents state that 15% to 20% of annual budget has been set aside for I.C.T.. Only 0.6% respondents state that 20% and above of annual budget is set aside for I.C.T. (Ref Table 4.52). But on an average only 19.88% of Annual Budget is set aside for I.C.T. (Ref- Table 4.53) as per Teaching Staff. As compared to estimated recurring and Non-recurring expenses regarding I.C.T., only 0.6% respondents stating that 20% and above of annual budget is set aside for I.C.T. is too low and means that even though institutions are charging development fee from students they are not investing it in I.C.T. infrastructure. The average as per technical staff is only 19.88%.

- As per Teaching Staff (ignoring Can’t Say responses), the highest responses have been received by 20% to 40% of sanctioned I.C.T. budget (14.2%). 6.9% say their institute uses 40% to 60% of sanctioned I.C.T. budget. Only 0.3% say that their institution is using 80% and above of sanctioned I.C.T. budget. (Ref Table 4.54). Only 0.3% institutions using 80% and above of allocated for I.C.T. is a very critical issue. Though provision has been made in budget but these funds are lying unutilized. Thus, users have to work on old PCs and the network is also not ready to handle ever increasing security threats.

- As per Teaching Staff, 87.95% of these respondents have given positive response for “Investment in I.C.T. is every Penny Worth”. Of these 16.57% say that they Agree with it while 71.39% say that they Strongly Agree with it. (Ref Table 4.56). Majority of Full-Time Teaching Staff Agree (87.95%) that “Investment in I.C.T. is every Penny Worth”. This means that they known and understand the importance of I.C.T. in academics and are very sure about its positive outcomes.

- As per Full-Time Teaching Staff, Research (4.72; 97.6% agree responses) and Communication (4.66; 96.7% agree responses) have given highest benefits or maximum Return of Investments on I.C.T. and have Ranked FIRST and
SECOND. *Examination process* lands at FOURTH rank with 96.39% positive responses. Stationary (e.g. paperless office) is at the bottom of the list with only 50.30% positive responses. In fact there is no item in the list which has received negative responses from the Teaching Staff respondents. (Ref Table 4.59) Majority of Full-Time Teaching Staff agree that Research and Communications are areas where maximum benefits have been attained by investing in I.C.T.. But, though, the responses for Stationary are positive but approx. 50% is quite low. This means that as per Teaching Staff even after introduction of I.C.T., the academic institutions are still not able to cut-down the spending on Stationary which might be for examination, record keeping, etc.

- As per Full-Time Teaching Staff, *Knowledge Sharing* and *Maximize resource utilization including learning resources* are the benefits which Rank at FIRST and SECOND position in the list of Benefits provided by implementation of I.C.T. in higher technical. They have attained 96.99% and 98.19% positive AGREE responses respectively.

*Reduced need of direct attention* with 46.08% positive Agree responses and *Reduced labour costs* with 47.6% positive responses for Agree come at the last of the list. (Ref Table- 4.64) *We can thus conclude that Teaching Staff doesn’t think that introduction of I.C.T. in higher technical educational institutions have benefited with introduction of I.C.T. in the field of reduction of direct attention and Reduction in labour costs.*

### 5.1.3 PART III: FINDINGS FROM FULL-TIME STUDENTS:

Full-Time Students constitutes the majority part of the end-users of I.C.T. infrastructure and facilities in institutions of Higher Technical Education. It is these students which form the majority of users of I.C.T. infrastructure in any Higher Technical Institution. They use the machines in the Computer labs. They give presentations and lectures using PPT presentations etc. In fact it is these students who are the customers of the institution and the biggest critics of facilities offered by these institutions. Thus, their opinion regarding various facets of I.C.T. infrastructure and services offered in institution of service is quite important.
For this type of respondent type of primary data was collected using questionnaires from 435 respondents who were enrolled as Full-time Students at Professional higher technical education institution running A.I.C.T.E. approved course and teaching only A.I.C.T.E. approved course.

In this case the data collection collected and analyzed based on following points (excluding certain general institute-related information) viz. Total Number of Full-time enrolled Students (including all years), Courses Conducted (A.I.C.T.E. Approved only), Total PCs, Availability Laptops, printers, etc. available to students and staff for use, Software Type used the institution (Open-source, licensed, etc.), Purpose of using institution’s I.C.T. infrastructure, Extent of satisfaction w.r.t. to I.C.T. services by the institution, Extent of satisfaction w.r.t overall I.C.T. infrastructure security, Extent of satisfaction w.r.t overall I.C.T. Digital assets security, Identify I.C.T. security lapses, Areas for improvement in I.C.T. security.

- As per Full-time Student Respondent’s views (Refer Table 4.9), PCs have been Ranked at No. 1 (93.1% frequently available for use) followed by Printers (Rank 2; 34.2% frequently available for use), Scanners (Rank 3; 90.6% frequently not available for use), Laptops (Rank 4; 91.7% frequently not available for use). This implies that according to Full-time Students, the institutions where they are studying, PCs are most available for users. Deeper analysis shows that Printers, Scanners and Laptops have received negative responses for availability at 65.5%, 90.6% and 91.7%. (Ref Table- 4.6). As per Full-Time Students, PCs are available for their use at their educational institute, but on the other hand, Printers, Scanners and Laptops are not available for use for students. The institution might be owning these equipment but they don’t allow students to use them.

- As per Full-Time student responses with regards to type of software available in institutions (Ref Table 4.14), most frequently available is Licensed Software with 72.90% respondents giving Positive response for Frequently available. This is followed by Open-Source Software (76.80% positive responses). In-house software are at the bottom of the list where only 4.80% respondents have given positive responses for frequently available. Students have also said that trial-
version software are also quite frequently used with 77.80% positive responses for frequently available. As per Full-Time Students responses, Licensed software are the most commonly available software type followed by Open-source. They have also suggested that Trial version software are very commonly used. This is not good from both legal and I.C.T. security point of view. Also, their response points out those institutions are neither developing nor using in-house developed software. This is waste of talent and experience of teaching staff and students (in particular those belonging to Computer related courses).

- As per Full-Time student responses with regards to purpose for which they use their institution’s I.C.T. infrastructure (Ref. Table 4.20), the most frequent one is Email (Rank FIRST) with 90.11% positive responses for frequent use. This is followed by Lecture and practical sessions (Rank SECOND) with 79.31% positive responses for frequently used. Social Networking (Rank THIRD) 77.24% positive responses for frequently used.

As per Full-time student responses we find that, Presence of Email on Rank 1st and Social Networking on Rank 3rd on one hand while View Online Lectures and Vocational Training appearing at 11th and 12th Ranks respectively which means Students don’t use I.C.T. infrastructure for academic purposes or for self-development. The Student’s usage pattern depicts that students are more inclined towards entertainment and socializing and that academics is their second preference w.r.t. using their institute’s I.C.T. infrastructure.

- As per Full-Time Student Respondent’s views regarding satisfaction with certain I.C.T. services (Refer Table 4.26), Communication facilities (email, SMS, alert messaging, etc.) has Ranked at No. 1 (84.6% Satisfied responses) followed by Internet services through wired network (Rank 2; 62.8% Satisfied responses) and show weighted averages that correspond to Satisfied. Academic application software (Rank 3; 60.5% Satisfied responses) and Internet services through Wi-Fi (Rank 4; 46.4% Satisfied responses) show weighted averages that correspond to Neutral. Storage and Backup utilities and Administration software Rank at 7th and 8th also show weighted averages corresponding to Neutral. Further analysis
show that in case of Storage and Backup utilities the number of respondents who are Dissatisfied (53.80%) far exceeds the number of respondents that are Satisfied (37.20%). This implies that respondents are actually Dissatisfied with it. Full-Time Students are not satisfied with Storage and back-up utilities and Administration Software. This means that institutions especially the big ones should build dedicated data storage facilities including Storage Area Networks.

- As per Full-Time Student Respondent’s views regarding Measures to improve User Satisfaction w.r.t. I.C.T. Services provided by Institutions, Anti-virus (92.2%) is most required. This is followed by Increase Internet bandwidth and making available on all PCs(91%) and Training of Technical support staff (78.2%). More Frequent updating of organization’s I.C.T. Security Policy in consultation with stakeholders including staff and students,(41.6%) is least required as per Full-Time Students. Under Others, Students have asked for Free academic software for installation on their own personal PCs / laptops which they need for study purpose (Ref Table 4.28). Full-Time Students want Antivirus to be installed on all PCs which means that students have found that antivirus are not installed on PCs available for their usage in the institute. They also want an increase in Internet bandwidth. They need trained I.C.T. Technical Support Staff which means that either institutes do not have adequate technical staff or they are not skilled enough to maintain the I.C.T. infrastructure. Most of the students feel that their inputs in I.C.T. security policy drafting will not much effect the satisfaction.

- Full-Time Student responses have shown that they are Satisfied with The overall I.C.T. Infrastructure Security with Weighted Avg. 3.67 and nearly 78% showing positive responses for Satisfied (Ref Table 4.30). Majority of Full-Time Students are in general Satisfied with overall I.C.T. infrastructure Security.

- Majority Full-Time Student responses have shown that they Can’t Say much about The overall I.C.T. Digital assets security with Weighted Avg. 2.94 but ignoring Can’t and Neutral responses13.30% have positive responses for Satisfied while 17.50% have shown negative responses w.r.t. overall I.C.T.
Digital Security(Ref Table 4.32). **Full-Time Students are Not Satisfied with overall I.C.T. Digital Security.**

- With respect to certain points which highlight the I.C.T. security scenario in Higher Technical Education Institutions, the Full-Time Student responses point out that 2 factors namely *I.C.T. security policy displayed in labs and prominent areas the institution, Have you ever been educated about your institution’s I.C.T. Policy* where respondent’s given more NO responses 57.01% and 62.30% respectively.

Also, 79.3% respondents said they were able to install any software on their institution’s PCs. Again, when it came to *Sharing I.C.T. username (e.g. internet, file drive) with friend*, 58.6% respondents said that they have done so. Similarly, 57.2% respondents have stated that their *data was destroyed by virus from the PCs or pen drives, etc. while they were accessing it on Institute’s PC.*

**Full-Time Students have pointed out that majority institutions either might not have a formally drafted I.C.T. security policy or they have failed to display it to general public users due to which students might not be aware of the existence of an I.C.T. security policy. This is a bad situation because if students have not been educated or enlightened about the various rules for I.C.T. usage covered under I.C.T. security policy, then how will they understand what they should do and what they shouldn’t when using institution’s I.C.T. infrastructure and services. Students have also revealed that they have shared their I.C.T. usernames with their friends and also that many times their data has been destroyed due to virus on institute’s PCs.**

- With Respect to Areas to be addresses to improve I.C.T. security in the institutes, The foremost area suggested by Full-Time Students is *User Awareness about cyber laws* (87.6%). This is followed by *Train users to identify I.C.T. security risks* (86%). Stringent penalties (27%) is least favored area. (Ref Table 4.49). **Full-Time Students opinion w.r.t. Areas to be addresses to improve I.C.T. security in the institutes is more inclined towards educating the users about the cyber laws and creating awareness among the users regarding identification of potential areas which could create a breach in**
I.C.T. security. They do not favour any stringent on Users or technical Staff or any other staff on the institute to be used as a mean to forceful means to improve I.C.T. security.

5.1.4 PART IV: FINDINGS FROM HEAD OF INSTITUTE:

Head of Institution is one of the main administrative and decision making authority in institutions of Higher Technical Education. Thus, their opinion regarding various facets of I.C.T. infrastructure and services including policy decisions, budgetary decisions, etc.

For this type of respondent type of primary data was collected using questionnaires from 38 respondents who were either owners of institutions or were working as full-time paid Directors / Principals / HoD, etc. at Professional higher technical education institution running A.I.C.T.E. approved course and teaching only A.I.C.T.E. approved course.

In this case the data collection collected and analyzed based on following points (excluding certain general institute-related information) viz.Total Number of Staff members, Norms followed for creating your I.C.T. infrastructure, I.C.T. implementation support source, Total Number of PCs , Total number of Support Staff, Type of PCs and Servers, Internet Speed, Extent of satisfaction w.r.t overall I.C.T. infrastructure security, Extent of satisfaction w.r.t. overall I.C.T. Digital assets security, Level of I.C.T. attacks encountered, Role in I.C.T. Security Policy framing, Presence of I.C.T. up-gradation policy, Licensed Antivirus software available of PCs and Servers, Percentage of Annual Budget is set aside for I.C.T. and Actual expenditure Percentage made on New purchases / Up-gradation of I.C.T., Whether investment in I.C.T. infrastructure is every penny worth spent, Areas providing benefits and maximum Return of Investments on I.C.T..

- As per Head of Institute respondents (Ref Table- 4.2), Vendor Support (94.7%) has been most highly used sources for I.C.T. implementation in their educational institutions of higher professional education. This is followed by Internal Sources (60.2%). Head of Institute respondents state that their institute have mostly used Vendor Support and Internal Source (staff) for setting-up and maintenance.
As per Head of Institute respondents (Ref Table- 4.5), A.I.C.T.E. Norms (100%) have been mostly followed by Affiliating University Norms (73.7%) and DTE Norms (65.8%) whereas UGC Norms (28.9%) has been least followed for creating I.C.T. infrastructure. **Head of Institute respondents state that in their institute A.I.C.T.E. Norms and Affiliating University are most followed for creating I.C.T. infrastructure but UGC Norms are least followed. A.I.C.T.E. norms being followed by majority of institutes is good but this needs to be verified. UGC norms is least followed but one reason for this is that UGC norms are not directly followed by individual institutions but by Universities.**

63.2% of Head of Institute respondents state that their institute uses only Branded Servers and PCs while 36.8% state that their institute uses both Branded and non-branded ones. 0% respondents stated that their institute uses Non-Branded Servers and PCs (Ref Table 4.10). **As per Head of Institute respondents, no institute uses Non-Branded PCs and Servers. Majority have stated to have been using Only Branded PCs and Servers. This ensures quality of installed I.C.T. infrastructure coupled with security of infrastructure and data.**

Head of Institute’s responses show that they are Strongly Satisfied (4.66) with overall I.C.T. infrastructure security with 100% positive responses for satisfaction (Ref Table- 4.30). **Head of Institute respondents are very Satisfied with I.C.T. infrastructure security.**

Head of Institute’s responses show that they are Strongly Satisfied with overall I.C.T. Digital assets security with majority of the respondents (94.8%) showing positive responses for satisfaction (Ref Table- 4.32). **Head of Institute respondents are very Satisfied with overall I.C.T. Digital assets security.**

As per Head of Institute respondents (Ref Table 4.36), Low intensity attacks (1.92- Moderately low occurrence) is most frequently occurring followed by Mild (1.34-very low occurrence) and (1.05- very low occurrence). **This means that as per Head of institute respondents though Low, mild and high attacks...**
are also occurring but their frequently occurring is very low. Of the three it is the Low intensity attacks which is most occurring.

- Head of Institute’s responses depict that their role is majorly as Final Decision Maker (76.3%) when it comes to role a respondent plays in creating I.C.T. policy. (Ref Table). **Majority of Head of Institute respondents are Final Decision Maker when it comes to I.C.T. policy making.**

- 39.5% of the Head of Institute state that Formal I.C.T. Up-gradation policy is not present while 36.8% say it is present in their institution (Ref Table 4.45). As per Head of Institutes majority of institutions do not have a formal drafted I.C.T. Up-gradation policy. This means that there is no planned upgradation in I.C.T. infrastructure. Upgradation decision will thus depend on priority and need along with the perception of the need in the eyes of the head of Institution who is final decision maker in financial matters.

- 65.8% Head of Institute state that All Servers have antivirus installed on them while 34.2% state that Few Servers have antivirus installed on them. This means that majority of servers are protected by antivirus. On the other hand, 44.7% Head of Institute respondents state that All PCs have antivirus installed on them whereas 55.3% state that Few PCs have antivirus installed on them (Ref Table 4.32). **As per Head of institute respondents, majority institutes have antivirus installed on all servers but when it comes to PCs majority of institutions do not have antivirus installed on all PCs but instead on few machines. Thus, in considerable number of cases, considerable number of PCs not are protected by antivirus.**

- When it comes to Percentage of Annual Budget set aside for I.C.T., The highest responses from Head of Institute (36.8%) is for 15% to 20% of annual budget set aside for I.C.T. followed by 26.3% for 20% and Above. (Ref Table 4.52). But on an average only 17.98% of Annual Budget is set aside for I.C.T. (Ref- Table 4.53) as per Head of Institute respondents. **As per Head of Institute responses, majority institutes dedicate only 15% to 20% of their Annual Budget for I.C.T. and the avg. percentage of I.C.T. budget is 17.98%.**
As per Head of Institute, highest responses have been received by 60% to 80% of sanctioned I.C.T. budget (36.8%). Only 21.1% respondents say that 80% and above of sanctioned I.C.T. budget is being actually used by the institutes. (Ref Table- 4.54). As per Head of Institute respondent responses only 21.1% institutions are using 80% or more of the budget allocated for I.C.T..

Ref Table 4.56, Head of Institute (100%).have Strongly Agree upon the statement “Investment in I.C.T. infrastructure is every penny worth spent”. All Head of Institute Strongly Agree upon the statement “Investment in I.C.T. infrastructure is every penny worth spent”.

As per Head of Institute Respondent’s views (Refer Table 4.60), Communication has Ranked at No. 1 (100% High Return responses) followed by Research (Rank 2; 100% High Return responses), and Stationary (e.g. paperless office) (Rank 3; 100% High Return responses) and show weighted averages that correspond to Very High Return. In fact, all areas under study have shown trends of Very High Returns as per Head of Institute Respondents expect for Automation and integration Manpower (Teaching, Non-teaching, etc.) staff and Others which have showed trends of High returns. As per Head of Institute respondents all areas under study have shown good amount of benefits / Return on Investments. Of these Communication and Research (both 100% high return responses) are the areas which gives maximum benefits. Manpower (Teaching, Non-teaching, etc.) staff comes last in the list.

As per Head of Institute Respondent’s views (Refer Table 4.65), Knowledge Sharing, Effective communication between staff, students and other stakeholders, Reduction in teaching-learning costs, Increase in admissions have same Weighted Averages and actually share the Rank No. 1 (Avg. weight- 4.97; 100% Agree responses) and shows weighted averages corresponding to Strongly Agree.Attract more students and expert faculty members, Staff Skill development, and Reduced administrative costs rank at No. 2 (Avg. weight- 4.97). Facility rentals for corporate training and online exams (Avg. weight- 3.79) ranks last but has weighted average corresponding to Agree. As per Head of Institute respondents all listed items have given High benefits. Of these Knowledge Sharing, Effective communication between staff, students and other
stakeholders, Reduction in teaching-learning costs, Increase in admissions have shown highest benefits. Though Facility rentals for corporate training and online exams has also shown to be beneficial but it has been placed at the bottom of the list.

5.1.5 PART V: OVERALL FINDINGS:

A total number of 38 Head of Institute (Management) respondents, 332 Full-time teaching staff respondents, 435 Full-time students (Learners) respondents and 111 Technical Support Staff respondents were used to collect Primary data for the purpose of obtaining the objectives of the study. In this section we look at the overall response trends of the various respondents taken together for obtaining an overall view regarding the various factors under study for each objective type.

- Overall, majority of institutions having Upto 300 students have the minimum required number of PCs. In fact, 36.7% institutions having upto 300 students have even more than 150 PCs. 66.7% institutions falling in the range of 300 to 600 students have only minimum 150 PCs. While only 33.3% institutions have the required or amount of PCs. 36.8% institutions falling in the range of 300 to 600 students have less than minimum of 300 PCs. 52.6% institutions have the required amount of minimum 300 PCs while 10.5% institutions have more than the required amount of PCs. (Ref Table 4.2). Overall, majority of the institutes with less (upto 150 students) have been found to have minimum or higher number of PCs than required. The trends indicate that as the institutions grow and increase their intake, of students they fail to increase the number of PCs required as per norms. But once their intake crosses 600 students the situation improves.

- Overall, Vendor Support (87.92%) has been most commonly used for I.C.T. implementation in the educational institutions of higher professional education. Second choice has been the Internal Sources (46.98%). The least chosen one is Large general consulting firm (22.82%). (Ref Table 4.4). Overall, most preferred or used source of I.C.T. implementation is Vendor Support followed by Internal Sources. Large general consulting firm and Independent specialist consultants are least preferred which makes us conclude that there is a wide difference in attitude of higher education.
institutes and Industry when it comes to I.C.T. infrastructure implementation.

- Overall it is the *A.I.C.T.E. Norms* (74.49%) which have been most commonly been followed to create I.C.T. infrastructure. This is followed by *Affiliating University Norms* (49.44%). *(Ref Table 4.6)*. **Overall most commonly followed norms for creating I.C.T. infrastructure is A.I.C.T.E. norms followed by Affiliating University norms.**

- Overall, *Branded PCs and Servers* (67%) are most commonly available in higher technical education institutes while those using a mix of Both Branded and Non-Branded PCs and Servers (32%) come on the second place. *(Ref Table 4.11)* **Overall majority of institutes use Branded PCs and Servers.**

- *In-House developed software are not frequently used.*

- For 300 to 600 students, minimum internet bandwidth requirement is 5 Mpbs. 33.33% have bandwidth between 5 to 10 Mbps while 58.3% have 10 Mbps and above. For the student range of 1200 to 1500 students, the minimum required bandwidth is 10 mbps. Only 28.6% institutions in this range has subscribed this bandwidth while 71.4% institutions have subscribed internet bandwidth below this minimum level. *(Ref Table 14.13a). Overall, when institution’s intake is less the required internet bandwidth subscription is available and in some cases even more but the institutions which have enrolled students in the range of 1200 to 1500 must have atleast 10 Mbps internet speed but only 28.6% institutes have it.**

- Overall, Broadband (51.4%) tops the list as most commonly used Internet connection type followed by Leased-line (48.6%). Other traditional types of connections like ISDN and Dial-Up are not at all being used. *(Ref Table 4.17). Overall, most commonly used connection type by higher technical education institutes is Broadband followed Leasedline. ISDN and Dial-up connections are no longer preferred.**

- As per Technical and Teaching Staff combined responses *Research Work* (4.46) is the most common purpose for the usage of I.C.T. infrastructure in Higher
technical Education Institutions and is Ranked **FIRST** and show tendency of **Very Frequently used**. Email (4.38) is ranked **Second** whereas Lecture Preparation (4.10) has been ranked **Third**. Both show tendency of Frequently used. Job Searching (2.25) and Listening to Songs and Videos (2.18) is the least preferred purposed as per combined view of technical and teaching Staff. For Students the main purpose for use is Email, lecture and practical sessions, & Social Networking. Least used purposes are View Online Lectures and Vocational Training. (Ref Table 4.21 and Table 4.22). As per Technical and teaching staff, Research Work, Email and Lecture are most common purposes for which I.C.T. infrastructure of educational institute is used. Contrary to this, Job Searching and Listening to songs and videos is least used. While Teaching Staff’s usage pattern depicts their inclination towards usage of I.C.T. infrastructure for academic purpose, the Student’s usage pattern depicts that students are more inclined towards entertainment and socializing and that academics is their second preference w.r.t. using their institute’s I.C.T. infrastructure.

- (Ref Table 4.22) Overall, majority of institutions are Not Connected with ERNET (48.6%). One reason for this is that ERNET is not available to private educational institutions. That is also the reason why a lot of Technical Staff respondents are not aware of its existence.

- Overall (Refer Table 4.23), 86.49% respondents say that their institution has Wi-Fi network installed while only 13.51% respondents say that their institution doesn’t have Wi-Fi network installed. Overall, majority of the institutions have Wi-Fi network installed in their building / campus. This is good indication but it is not clear whether Wi-Fi internet availability is allowed for students or it is just limited to usage by Staff and Management.

- Overall, Communication facilities (email, SMS, alert messaging, etc.) is Ranked **First** (4.27) w.r.t. Satisfaction trends among users. This is followed by Internet services through wired network (3.91) and Academic application software (3.65) at Second and Third Ranks respectively. All three of them show trends of Satisfied. Storage and Backup utilities (2.86) ranks at Eighth position and end at the bottom of the list. (Ref Table 4.27). Overall, as per respondents the top-
most I.C.T. services with which respondents are satisfied are Communication facilities, and internet through wired network. Academic software are also available in institutions. But Internet through Wi-Fi is not in top 3 list. Also data Backup and Storage facility is right at the bottom of the list. This indicates that (i) Wi-Fi internet might be present in the institution but access might be available to only select few classes of users. (ii) Institutions are lacking in having properly managed Data storage and Backup facilities. Academic and financial records are at the heart of an academic institution. As we are moving towards digitization and moving away from Paper-based record keeping, lack of data backup facilities can be catastrophic.

- Overall, the most highly desired measure to improve user satisfaction as per all types of respondents is Antivirus(91.80%), Training of technical support staff(79.04%) and Increase Internet bandwidth and making available on all PCs(79.04%). More Frequent updating of organization’s I.C.T. Security Policy in consultation with stakeholders including staff and students (55.47%) is the least required improvement area desired by respondents collectively. (Ref Table 4.29). Overall most desired measures to improve user satisfaction is installation of Antivirus on PCs and Servers followed by Training of technical support staff and Increase Internet bandwidth and making available on all PCs. More Frequent updating of organization’s I.C.T. Security Policy in consultation with stakeholders including staff and students is least preferred.

- Overall, the respondents are Satisfied (Combined Weighted Avg. 3.87) with the I.C.T. infrastructure security being maintained in Higher Technical Education in Pune region. (Ref Table 4.31). Overall all respondents have shown that they are satisfied with overall I.C.T. infrastructure Security. But we must remember that I.C.T. security must be maintained at its peak i.e. responses should show Very Satisfied levels but this not so. Even slight lapse in security can compromise security of valuable data. Therefore, researcher infers that more need to be done to reach the Very Satisfied level.
Overall responses of all respondents taken together reveal that the users have not given a very clear picture regarding whether they are satisfied or not with overall I.C.T. Digital assets security. The value of Combined Weighted Average (3.41) is more inclined towards Neutral. Further analysis has revealed that Technical Staff and Head of Institute are satisfied with Overall I.C.T. Digital assets security but it is possible that their response could be biased as both are directly linked to I.C.T. security aspect as owners/service providers. On the other hand, Students who are the end-users are actually dissatisfied. We must take in mind that the Students are in majority in the category of end-users and their dissatisfaction must be taken into consideration. (Ref Table 4.33). Overall, the combined Weighted Avg. shows results which are closer to Neutral trends w.r.t. overall I.C.T. Digital assets security. But deeper analysis shows even though individually Technical Staff and Head of Institution show trends of Satisfaction but Students have shown trends of Dissatisfaction.

Overall The Combined Weighted Average for Low Intensity (2.35) infers that Low intensity attacks have Moderately Low rate of occurrence on overall basis (Ref Table 4.37). The Combined Weighted Average for Mild Intensity (1.67) infers that Mild intensity attacks have Moderately Low rate of occurrence on overall basis. (Ref Table 4.38). The Combined Weighted Average for High Intensity (1.46) infers that High intensity attacks have Moderately Low rate of occurrence on overall basis (Ref Table 4.39). Overall, Low Intensity attacks have more frequency of occurrence than Mild and High ones. It has been found that lots of I.C.T. attacks that happen in higher educational institutions have students involved in it who either try to create attacks for fun or as a challenge, etc. This is a common trend in countries like USA but India is still lagging behind. We must understand that Indian students are still raw and lack technical skills but in future as the generations of students change and their technical skills are enhanced, these figures which are, as of now, for Low Intensity attacks might change into those for High Intensity attacks. There is one more important fact that needs to be considered. Still there are lots of academic institutions in India who have not brought all their servers and data fully online that’s why hackers and attackers might
have not have been attracted to attack them. But as they will be digitized High Intensity attacks may well occur there also.

- Head of Institute’s responses depict that their role is majorly as Final Decision Maker (76.3%) while Technical Staff’s responses depict that majority of these respondent’s role in Policy Making is confined to Consultative (82.9%). (Ref Table 4.40). Overall w.r.t. Role in I.C.T. policy making, I.C.T. Technical Staff is more into giving Consultancy while Head of Institutes are the Final decision makers

- Overall w.r.t. Presence of formal I.C.T. Up-gradation Policy in the higher technical education institution, only 23.28% respondents have given a YES response where as 37.21% have given NO response. 39.50% have given Can’t say responses and have, therefore, been omitted (Ref Table 4.42). **Overall, only 23.28% respondents have stated that their institution has aFormal I.C.T. Up-gradation Policy while majority have stated that it is not present.**

- Overall in case of Servers, 56.38% respondents say it is installed on all Servers whereas 40.94% say it is installed on few servers in their technical higher educational institution. Overall, in case of PCs, 34.23% respondents have opined that antivirus is installed on All PCs, but on the other hand 65.77% say that it is installed on Few PCs. (Ref Table 4.44). **Overall, Majority of respondents have reported to have antivirus installed on all Servers. But in case of PCs in most cases on an average the antivirus is not installed on all PCs in the institution. Further, in both cases, it is seen that Antivirus is installed on Few Servers and Few PCs (majority in case of PCs). But we are not clear about the exact percentage of machines when we are dealing with the term “FEW”. Thus, if in case, the percentage of antivirus installed machines (Servers and PCs) is in minority then this is not a good trend as servers are the machines where majority data is stored or they provide vital network services and if they are not secured then it is a problem worth noting. One of the biggest threats to data in academic institutions comes from students who work on public PCs available in computer labs of their academic institutions. Lack of antivirus on such public computers is very bad for the security of data in such institutions.**
Overall, **Lack of Technical staff, Carelessness of users, Lack of equipment / technology / software in the institution to avoid I.C.T. attacks** Ranked I, II and III and showed weighted average corresponding to High Role as Factors which play major role in committing of I.C.T. security attacks. **Lack of hardware / data, etc. disposal policy, Lack of Content management, Lack of Data Governance (Management/storage/dispersion) policy, and Lack of fixation of responsibility and liabilities on users** which are ranked at 14th, 15th, 16th and 17th rank show weighted averages which correspond to neutral responses from respondents. Another factor of interest is **Pirated software** where 90.09% respondents have stated that it plays High Role in committing of I.C.T. Security attacks. There are some other factors also which have been stated by Respondents in Others category which are of interest. Some of these factors include Allowing students to access internet on Mobile smart phones, **Allowing students to use Pen drives on PCs, Exchanging user passwords by users with other users, Careless of users while browsing internet which causes installing of Spyware and Adware, No antivirus on machines, Antivirus not updating its virus database, etc.** Researcher also came across a peculiar case where respondents said that their **Lab PCs had antivirus but there was no regular internet in labs to update them.** (Ref Table 4.45). Overall, factors which play highest role in committing I.C.T. security attacks are **Lack of Technical staff, Carelessness of users, Lack of equipment / technology / software in the institution to avoid I.C.T. attacks. Lack of Data Governance (Management/storage/dispersion) policy, and Lack of fixation of responsibility and liabilities on users** are last in the list. Other reasons sited are Allowing students to access internet on Mobile smart phones, **Allowing students to use Pen drives on PCs, Exchanging user passwords by users with other users, Careless of users while browsing internet which causes installing of Spyware and Adware, No antivirus on machines, Antivirus not updating its virus database, etc.**

Overall the top most factors which might be playing high role in reducing/preventing I.C.T. security attacks are **Technical staff able to manage I.C.T. infrastructure and its security** ranks **First** and falls under **High Role**, followed by **Antivirus, firewall, auto-updates, etc.** ranks **Second**, and **Educating of staff and students about I.C.T. laws and Best Practices** ranks **Third**.
Third. All these fall under Average role.(Ref Table 4.48). Overall Technical staff able to manage I.C.T. infrastructure and its security and Antivirus, firewall, auto-updates, etc. are the factors that respondents feel have played most important role in curbing I.C.T. security attacks in institutions of Higher Technical education.

- Overall, User Awareness about cyber laws (85.65%), Train users to identify I.C.T. security risks (84.05%), and Identification and blocking loopholes in security (80.52%) are the top-most Areas need to be addressed to improve I.C.T. security in the institutes. Whereas Stringent penalties are least related as per combined responses of all respondents.(Ref Table 4.50). Overall User Awareness about cyber laws, Train users to identify I.C.T. security risks and Identification and blocking loopholes in security most top rated Areas need to be addresses to improve I.C.T. security in the institutes. Respondents are not in favour of using Stringent Penalties as a way to improve I.C.T. security.

- Overall, I.C.T. security policy displayed in labs and prominent areas the institution, and, Have you ever been educated about your institution’s I.C.T. Policy where respondents have given more NO responses 57.01% and 62.30% respectively. This means that institutions might not have a formally drafted I.C.T. security policy or they have failed to display it to general public users. (Ref Table 4.51). Overall, it has been found that I.C.T. security policy displayed in labs and prominent areas the institution is not displayed, and users have not been educated about your institution’s I.C.T. Policy. These are two very big loopholes in the I.C.T. security in higher Technical education institutions.

- Overall, most institutions are allotting at an average of only 18.13% of their total annual budget for I.C.T.. (Ref Table 4.53). Overall, Very small percentage of Total Annual Budget of the Higher Technical Education Institution is being allocated for I.C.T..

- Overall, it can be inferred that most institutions are actually spending only 53.14% of their total Annual Budget set aside for New Purchases / Up-gradation
of I.C.T. (Ref Table 4.55). Overall, approximately 50% of the total Annual Budget set aside for New Purchases / Up-gradation of I.C.T. by Higher Technical Education Institution is being allocated for I.C.T. is actually used.

- The combined weighted average of 4.57 indicates that on overall respondents Strongly Agree to the statement that “Investment in I.C.T. infrastructure is every penny worth spent” (Ref Table 4.57). Overall the statement “Investment in I.C.T. infrastructure is every penny worth spent” has been strongly agree to by all respondents taken together.

- Overall, Communication (4.56) and Research (4.54) are ranked First and Second respectively and respondents have Strongly Agreed upon this that these are have shown highest extent of benefits or Return of Investments on I.C.T. received from various areas as per responses of Head of Institute. It is interesting to see that Information storage and access (4.22), Examination process (4.10), Stationary e.g. paperless office (3.93) have landed at 4th, 6th and 9th Rank in the list. Though these have shown trends of Agree, still they have landed quite low in the list. (Ref Table 4.62). Overall, Communication and Research have given highest return or benefits from investment in I.C.T. by higher technical education institutions. There is still much return from areas like Information storage and access, Examination process, Stationary e.g. paperless office.

- Overall there is very high diversity between the opinions of various respondent types w.r.t. benefits provided by I.C.T. implementation in higher technical education institutions. (Ref Table 4.66). But as per combined weighted averages of all the respondents, we find that Knowledge Sharing (4.63[Strongly Agreed]) is the benefit which has been Ranked First. Effective communication between staff, students and other stakeholders (4.36), Maximize resource utilization including learning resources (4.35), and Standardize processes (4.35) come at Ranks Second, Third, and Four respectively. Facility rentals for corporate training and online exams, Reduced need of direct attention, Reduced labour costs have not been able to be very beneficial and have landed at the bottom of the list. (Ref Table 4.67). Overall Effective communication between staff, students and other stakeholders,
Maximize resource utilization including learning resources, and Standardize processes have proved to be most beneficial. But the benefits from Facility rentals for corporate training and online exams, Reduced need of direct attention, Reduced labour costs are not that much lucrative.

5.2 CONCLUSIONS:

After going through the data and analyzing and interpreting it, the researcher has come up with the following conclusions:

- **PC-Student ratio:** The Management colleges which have higher number of enrolled students i.e. more than 900 but less than 1200, in majority of cases have lesser number of PCs than required.

- **I.C.T. Implementation and maintenance Sources:** Most institutions rely on Vendors and Internal Staff for setting-up and maintaining I.C.T. infrastructure and its security. Unlike their industry counter-parts, they, in majority of cases, don’t use external Experts and Consultants. Looking at the current delicate situation in I.C.T. security along with continuing digitization of academic sector, this is a very volatile situation.

- **Norms followed for creating I.C.T. infrastructure:** Majority of the Institutions are following A.I.C.T.E. norms, the foremost agency to regulate higher technical education in India. But this is “majority” and not 100%. This means some institutions are somehow by-passing A.I.C.T.E. Norms. This is evident from section4.2.1 where management institutes with higher number of enrolled students were not having adequate number of PCs. Moreover, too many norms from too many regulatory and accreditation bodies creates problems for institutions from administrative and compliance point of view.

- **Availability of basic I.C.T. equipment to users:** PCs are available to users as per Technical staff, Teaching staff.. But when it comes to Printers, they are available to Staff members only. All users agree that Laptops and Scanners are not available. This means that printers are not being made available to student users whereas either institutes don’t have scanners and
printers or they provide it only to a select few. Therefore, we conclude that basic I.C.T. equipment and tools are only available in part to the users.

**Types of PCs and Servers available in institutions:** Majority of the respondents i.e. Technical Staff, Full-Time Teaching Staff, and Head of Institute state that Only *Branded PCs and Servers* are being used in their institution. Overall, also the majority is with *Branded PCs and Servers*. In contrast, Responses from all the 3 types of respondents clearly shows that there are very few institutions that are using *Non-Branded PCs and Servers* alone (less than 5%). This is a good indication because Branded PCs and Servers are obviously good in quality, trust worthy, last long and their performance is also much better than Non-Branded ones. The data is also safe. One drawback of this data is that that we can’t exactly say the ratio of Branded and un-branded PCs and Servers in cases where institution is using both Branded and Non-Branded PCs and Servers. Considerable number of institutions (25% to 50%) use such a combination. If ratio of Non-Branded is higher, then it is a matter of concern as non-branded ones are frequently of inferior quality with high failure rate.

**Type of Software Used:** Technical and Teaching staff responses indicate that Licensed Software are the most commonly used software. Open-Source software are also quite commonly used. Problem persists with Trial-Version software are also used in abundance, and In-house Developed software which are not very prevalently used. On one hand, Trail-Version software depict a great vulnerability w.r.t. I.C.T. attacks through virus, spyware, Trojans, etc., while on the other, less use of In-house developed software depicts institutions, especially those institutions which are running Technical courses in the field of computers, are not utilizing the skills of their staff and students to practically develop software which could give a good practical exposure to them.

**Internet Speed:** All institutions have internet which is as per the norms setup by A.I.C.T.E..
- Internet Connection Type: All institutes have internet connection. Of these Broadband and Leasedline are most common in use w.r.t. higher technical education institutes.

- Purpose for using I.C.T. infrastructure: It is evident that there is a sharp difference between the usage patterns of Students and teaching staff. While Teaching Staff’s usage pattern depicts their inclination towards usage of I.C.T. infrastructure for academic purpose, the Student’s usage pattern depicts that students are more inclined towards entertainment and socializing and that academics is their second preference w.r.t. using their institute’s I.C.T. infrastructure. Staff working in Teaching or technical areas do not like to waste their time in leisure work during working hours and prefer spending more time in Research work and institutional activities.

- Connection to ERNET: Majority of institutions are not connected with ERNET. One reason for this is that ERNET is not available to private educational institutions. That is also the reason why a lot of Technical Staff respondents are not aware of its existence.

- Wi-Fi Network in institute: Wi-Fi network is generally available in majority of Professional Higher Technical Education institutions.

- Satisfaction among users w.r.t. select I.C.T. services provided by Institution: With respect to select I.C.T. services provided by Institution, on the brighter side, Communication, Internet through wired Network, maintenance and Support, and Academic Software are frequently seen in the first 3 positions even though there is difference in perception of the 3 respondent types. Overall also the scenario is the same. This makes us conclude that respondents are very much satisfied with these services.

Again on the darker side, Storage and Backup utilities constantly appears at the bottom of the list and respondents have shown very low satisfaction in this case. This means that this facility is either not available at all or is not available to all users. Researcher must point out that, Academic and financial records are at the heart of an academic institution. As we are
moving towards digitization and moving away from Paper-based record keeping, lack of data backup facilities can be catastrophic.

Internet through Wi-Fi is yet another facility which failed to appear in top 3 facilities which means that Wi-Fi (ref point 11) even though it is available in majority of institutions but then it is either available for use of select few or there are connectivity/ low bandwidth issues.

- **Measures to improve User Satisfaction:** There is definitely a difference in opinions of different respondent types regarding what should be done to improve user satisfaction. However, *Antivirus* has been a common factor that has come in majority of case at the top. Apart from this, *Increase in number of technical support staff* is another factor which features at the top. Few of the suggestions for improvement as prescribed by the respondents include *24*24*7 printing facility, printing facility in hostels, on-line academic document ordering and verification system, centralized I.C.T. technical desk helpline, college providing copy of academic software to use at home*, etc.

- **User Satisfaction w.r.t. overall I.C.T. infrastructure security:** Majority of respondents are found to be satisfied with overall I.C.T. infrastructure security. Overall, also the respondents are satisfied.

- **User Satisfaction w.r.t. overall I.C.T. Digital assets security:** Majority of the teaching staff and Head of Institute are Satisfied with overall I.C.T. digital asset security. On the other hand, Students who are the end-users are actually dissatisfied. We must take in mind that the Students are in majority in the category of end-users and their dissatisfaction must be taken into consideration.

Overall responses of all respondents taken together reveals that the users have not given a very clear picture regarding whether they Satisfied or not. Firstly, it is possible that responses of Head of Institute or Teaching Staff could be biased as both are directly linked to I.C.T. security aspect as owners / service providers. Secondly, it could be possible that laboratory machines are not well maintained or are virus hit due to unavailability of
antivirus on lab PCs which lead to destruction of student’s data. Section 4.4.6 does indicate that in majority of institutions the antivirus is not installed on all PCs.

- **Severity and Frequency of I.C.T. security attacks:** Overall, Low Intensity attacks have more frequency of occurrence than Mild and High ones. It has been found that lots of I.C.T. attacks that happen in higher educational institutions have students involved in it who either try to create attacks for fun or as a challenge, etc. This is a common trend in countries like USA but India is still lagging behind. We must understand that Indian students are still raw and lack technical skills but in future as the generations of students change and their technical skills are enhanced, these figures which are, as of now, for Low Intensity attacks might change into those for High Intensity attacks. There is one more important fact that needs to be considered. Still there are lots of academic institutions in India who have not brought all their servers and data fully online that’s why hackers and attackers might have not have been attracted to attack them. But as they will be digitized High Intensity attacks may well occur there also.

- **Respondent’s Role in Policy Making:** Technical Staff, even though they are at the operational level in I.C.T. infrastructure and maintenance, are not the Final Decision Makers w.r.t. I.C.T. policy making. In majority of the cases, the Final decision vests with the Head of Institute on the institution who may or may not take advice of Technical Staff. If they don’t take advice then it can be treated as I.C.T. security gap as Head of Institute are not technical experts in the area of I.C.T. security. Thus, a potential problem area.

- **Presence of formal I.C.T. Up-gradation policy in the institution:** Overall, only 23.28% respondents state that formal I.C.T. Up-gradation policy in the institution. This is an alarming state with regards to I.C.T. security scenario. This is because as new technology is coming up, new ways to create I.C.T. security attacks are coming up. If the institutions don’t have formal up-gradation policy it means that they are not upgrading themselves win orderly manner and might fail to have enough technical
capability and infrastructure to combat future possible I.C.T. security attacks. We can, thus, infer that due to lack of I.C.T. Up-gradation policy, the academic institution data is under high security threat on one hand, whereas on the other hand, Institutions are not providing quality I.C.T. infrastructure to their students who pay high amount of fee.

- **Antivirus installed on Servers and PCs:** 40.94% (Antivirus Installed on few Servers) and 65.77 (Antivirus Installed on Few PCs) is not a good trend. Servers are the machines where majority data is stored or they provide vital network services and if they are not secured then it is a problem worth noting. Same way PCs without antivirus are potential points from where virus can enter the network. Basically, what is expected is that each and every PC and Server should have an antivirus.

- **Factors which play major role in committing of I.C.T. security attacks:**
  Lack of technical staff and carelessness of users has been found to be the top most factor for committing I.C.T. security attacks. Use of Pirated Software is another factor to look for. Lack of hardware / data, etc. disposal policy, Lack of Content management, Lack of Data Governance (Management/storage/dispersion) policy, and Lack of fixation of responsibility and liabilities on users have lesser role as per respondents. Other factors include Allowing students to access internet on Mobile smart phones, Allowing students to use Pen drives on PCs, Exchanging user passwords by users with other users, Careless of users while browsing internet which causes installing of Spyware and Adware, No antivirus on machines, Antivirus not updating its virus database, etc. and Antivirus on Lab PCs not regularly updated.

  It needs to be noted that each factor doesn’t by itself causes attacks or increases the risk of attacks but when one or more of them come together I.C.T. attacks become imminent.

- **Success extent of factors in being able to reduce / prevent I.C.T. security lapse or attack:** It is the Technical staff able to manage I.C.T. infrastructure and its security and Antivirus, firewall, auto-updates, etc.
which have been found to be most influencing factors in reducing / preventing I.C.T. Security attacks. Security audit able to find gaps in I.C.T. security has been found not to be very useful.

Researcher has also found that not too many institutions are conducting I.C.T. security Audits which is contrary to the practices followed in industry. This is evident from the fact that Security audit able to find gaps in I.C.T. security (2.48) has found to be least preferred.

Thus, it can be inferred that Technical staff able to manage I.C.T. infrastructure and its security and Antivirus, firewall, auto-updates, etc. are the factors that respondents feel have played most important role in curbing I.C.T. security attacks in institutions of Higher Technical education. Also in Indian context, Security audit has proved to be of no use as it is not conducted on regular basis.

- **Areas that need to be addressed to improve I.C.T. security in the institutes:** User Awareness about cyber laws is overall best solution for improvement in I.C.T. security. Stringent Penalties, which has highly demanded by Technical staff is not found to be acceptable by all other respondents.

- **Current I.C.T. scenario from Student User’s prospective**

  They data has been analyzed in Two parts:

  **Discrepancies found:**

  a. Only 43% students stated that Is I.C.T. security policy displayed in labs and prominent areas in the institution.

  b. Only 37.7% students stated that been educated about your institution’s I.C.T. POLICY.

  c. 79.3% students stated that they you able to install any software on your institute’s PCs
d. 57.2% students stated that their data was destroyed by virus from the PCs or pen drives, etc. while they were accessing it on your Institute’s PC.
e. 58.6% students stated that they shared their I.C.T. username (e.g. internet, file drive) with their friends.

**Positive aspect:**

a. 69.7% students said that they have been educated about Cyber laws (e.g. IT Act 2000, etc.) by your institution
b. 71.3% students stated that there is restriction on what is surf on the college internet
c. 5.3% students stated that institution’s Website was hacked.

This makes us conclude that, On the negative side, majority of students stated that I.C.T. security policy was not displayed in prominent areas of their institute. Majority of them also stated that they were not educated about the institution’s I.C.T. policy. Majority Students were able to install any software by themselves. They even shared their secret user names and passwords with their friends. These result are in line with another fact found that majority of students faced destruction of their data while working on it on institution’s I.C.T. network. Absence of I.C.T. security policy or user’s not knowing about its contents, might be because it is not displayed, is one of the biggest reasons why users indulge in activities (knowingly or unknowingly) which can lead to compromise in I.C.T. security.

A positive thing that has been observed majority institution’s website has not been hacked and that majority of the students have been educated about Cyber laws (e.g. IT Act 2000, etc.) by your institution where 69.7%.

- **Percentage of Annual Budget set aside for I.C.T.:** Costs related to I.C.T. include Recurring costs like internet bills, repair and maintenance, subscriptions for anti-virus, salaries for technical staff, upgrading of hardware and software, and Non-recurring costs like buying new hardware and software, creating computer labs and laying the network and electrical cables, etc. Both non-recurring and recurring costs are quite high. Increasing
dependency on I.C.T. has increased costs related to I.C.T.. An average of 18.13% of Annual budget looks quite small in such a scenario.

- **Percentage of Annual Budget set aside for New purchases / Upgradation of I.C.T. is actually used:** Overall, approximately 50% of the total Annual Budget set aside for New Purchases / Up-gradation of I.C.T. by Higher Technical Education Institution is being allocated for I.C.T. is actually used.

This is an alarming condition as this means that *Non-recurring and Recurring expenditures* on I.C.T. are not met which may lead to problems in buying anti-virus, firewalls, repairing / replacing old machines, etc. culminating in higher rate of network and machine failures, loss of data, etc.

- **Investment in I.C.T. infrastructure is every penny worth spent:** People have understood the importance of I.C.T. in education especially Professional Higher technical Education and have Strongly agreed that there are lots of benefits in investing in I.C.T. infrastructure in their educational institutions.

- **Extent of benefits or maximum Return on Investments on I.C.T.:** There is difference in perception of respondents w.r.t. areas which have given high return on investment in I.C.T.. However, Communication and Research have emerged as the winners. Presence of *Information storage and access* (4.22), *Examination process* (4.10), *Stationary e.g. paperless office* (3.93) low in the list makes us infer that digitization is still not fully done and that these have still not been able to reduce the monetaryexpenses involved in storage of data and saving huge amount of stationary spent in examination process.

- **Benefits provided by implementation of I.C.T. in higher technical education institution:** There is difference in perception of different types of respondents w.r.t. benefits provided by I.C.T.. However, *Knowledge Sharing, Effective communication between staff, students and other stakeholders, Maximize resource utilization including learning resources, Standardize processes, Increase in admissions have come in Top 5*. But these might have got majority positive responses but the results should be 100% effective.
SUMMARY OF CONCLUSIONS

To conclude, the researcher has found lots of positive points as well as negative points when talking about ICT facilities in Higher Technical Education institutes. There is a deficiency of PCs in certain types of institutes. This is also accompanied by the problem of having a number of different versions of norms being forced upon the Management of educational institutions by different accreditation and regulatory authorities. Continuous digitization of academic sector is taking place and not taking expert help in setting up ICT infrastructure is a cause of concern. Management is not allowing students to use printers, laptops and scanners even after paying a huge fee. Similar is the case with the Wi-Fi facility where Management is not allowing students to use the facility. These being the part of basic ICT facility is causing a lot of dissatisfaction among students. The Management of institutes at many instances has also failed to provide anti-virus on PC. The Management of institutes has also don’t have an ICT security policy, ICT audit policy, ICT Up-gradation policy and to make things worse, the budget for ICT is low and actual spending is even lower. There is also manpower shortage.

Still Management of institutes can’t be fully blamed. The government has also failed to mention certain specifications w.r.t. ICT facilities through its ICT regulatory authorities.

Benefits realized from ICT have also not gone well. Management of institutes as well as education regulators and universities should change their way of thinking and adopt online examination system and paperless culture (digitization of documents and office work). These two areas take up lot of time and money and must be worked upon.

If right policies and directives are in place, the Management of institutes will also be bound to implement these in their own policies and decisions and then only there will be satisfaction among the various users of ICT in institutions.

Looking at the summary, we can, thus, conclude that appropriate number of factors have been studied for this particular objective and so the study of this objective has been successfully completed.
5.3 SUGGESTIONS:

Looking at the conclusions of the study, the researcher wishes to present a number of suggestions which if practiced would definitely improve the situation.

The researcher hereby presents these suggestions in three parts:

i) There are Areas which are not at all doing well and are under performing.

ii) There are Areas which are doing well but then there is always a space for further improvement.

iii) The Framework

I) Areas which are not at all doing well and are under performing.

- There have been a deficiency of computers in Management strata where substantial number of institutes showing such a pattern. Such institutions must buy more PCs or they might rent them.

- Study has shown that certain institutions, though they say they are following all norms as devised by A.I.C.T.E., DTE, etc. but certain institutions somehow do manage to escape. These bodies can appoint a 3rd party to annually audit I.C.T. infrastructure in academic institutions. This trend is quite prevalent in industrial in areas such as quality control, compliance, etc.

- Too many norms from different regulatory and accreditation bodies causes chaos. Administrative and compliances issues make it difficult for the institution’s Management to comply with so many norms. One single body, preferably the UGC should make ICT related norms for all types of higher education institutions for pan-India. Later, AICTE, University, NBA, NAAC, etc. should all follow these norms only. Based on type of institution, like university or college, etc. the norms can be formed but by same apex body.

- Not all institutions specially those which are located in rural areas and/or are self-funding suffer financial problems in procuring expensive ICT
equipment. Relaxation should be made in norms for such institutes by the
government. Getting qualified staff to maintain the ICT setup is also a
problem. Grants for ICT infrastructure can be given by government through
UGC, AICTE, University, etc.

- Though Printers are available in institutions but students are unable to
  benefit from them in majority of the cases. As possible solution for this
  problem the Management of institutions can is to install network printers
  which are attached to labs. To keep control on wastage,a special software to
  manage printing can be installed and each student can be given a quota of
  certain number of pages for free print per semester or academic year. Beyond
  this quota the student can be made to pay at a subsidized per page rate.

- Management can procure Network Scanners are not easily available and the
  students don’t frequently use it. In such a case, at least one scanner needs to
  be installed on any one computer per lab or per floor where students can
  use it.

- Laptop availability is another area where the institutions are under-
  performing. No statutory norms also don’t mandate them. But all students
  don’t have PCs at their home and some might want to borrow them.
  Institutions can have a few laptops with them which through Library
  or I.C.T. department can give to students for a limited period of time.
  Damages done to the laptop can be recovered from students who are
  responsible for them by the Management.

- Use of Trial-version software is quite prevalent and institutions are unable
  to manage this. Even though institution’s staff know the repercussions of
  this, but students still install them. Few possible reasons for this are: lack of
  open-source software, expensive license for certain software, problem in
  security policy of PCs which lets users to install any software, etc. There no
  single solution to this. Management should have strong penalties in their
  ICT security policy for defaulter users. Management through Network
  administrators must make it a point of not allow software to be installed by
any other user other than the administrator using. This can be done by using group and local policies. Software manufacturers like Microsoft can give special limited period software license to students free or at subsidized prices through the institutions itself.

- There is an acute problem in the areas of Centralized Data Storage facilities. Nearly all universities and colleges in developed nations have one. Most Indian institutions don’t even have one except the IIMs, IITs, to name a few. A.I.C.T.E. and other education regulatory bodies can mandate the presence of this facility. Depending the size of the institutions different levels of centralized Data Storage facilities can be proposed. Universities and Technical Campuses can be mandated to have a Data Center.

- I.C.T. Security Policies are under performing which means that Management of Institute’s policies have failed when it comes to security. Management have either not been framed such policies or have not been implemented them properly. Student responses show that most colleges have failed to display them in relevant areas of the institution.

- I.C.T. Audit is one of the tools to make sure I.C.T. security policy is strictly implemented and can be used by both regulatory bodies and Institute’s Management for exercising control. Data collected from this research also shows that I.C.T. Audit has not been found to be of much use in prevention of I.C.T. attacks and that most institutions don’t even perform one periodically. Either Management of the institutes doesn’t conduct them or their findings are not taken seriously. None of the regulatory bodies mandates such type of an audit.

- Absence of Antivirus of PCs and Servers in Professional Higher Education Institutions is a problem. A.I.C.T.E. and other statutory educational regulatory authorities must make Antivirus compulsory for 100% PCs and Servers.

- The PCs which are for public use in labs have an average life of 4-5 years. Rough use and continuous changing requirements for installation of latest
software are important reasons for this. Absence of I.C.T. upgradation makes things worse. In countries like the USA, the PCs are changed every 3 years. Statutory Regulations must be made which mandate that all Higher Technical education institutions upgrade their PCs and Servers at regular intervals.

- The minimum hardware requirements in terms of R.A.M., Harddisk, Processor should be provided in detail by regulatory bodies. While deciding the same, the hardware and software requirements of the course must be kept in mind. Software used by Engineering and MCA need more processing power whereas Management and Pharmacy don’t need that much.

- There is lack of Hardware disposal policy. Old PCs and servers sold as scrap might contain hard disks which have vital data. Hardware disposal policy must include removal of the hard disk from Laptops, PCs and Servers before they are scrapped.

- As educational ERPs are still not installed / or not completely installed in all institutions especially small ones, data governance is a problem. A data governance policy needs to be created and should be implemented through ERP software so that RIGHT DATA is available to RIGHT PEOPLE at RIGHT TIME.

- I.C.T. security policy has not been able to play a major role in decreasing I.C.T. security attacks as per respondent’s opinion in the study. There are few reasons for this. Firstly, in many institutions there is no such policy. Secondly, if the policy is there it is not displayed for user reference or might be it’s contents are not effective or it is not actually implemented. I.C.T. policy need to be prepared compulsorily by Technical Staff after properly studying the requirements and taking feedback from all stakeholders. The policy needs to be displayed in all labs, classrooms and other relevant areas in the institutes. It must also mention the penalties for not following the provisions mentioned in it.
Responses have shown that I.C.T. has not shown much returns on investments in the area of examination process. The reason behind both these problems is that in India we are still more dependent of Paper based work. If Universities and institute’s Management conduct multiple choice questions pattern of examinations, the students will be bound to study more and depend less on low quality exam preparation guides to clear such exams. This will save teachers time w.r.t. answer books evaluation and will save paper stationary too.

To improve return on investments in information Storage and access, we need to improve ERP software and storage & backup utilities. Doing this will also help the management in taking decisions effectively.

II) Areas which are doing well but then there is always a space for further improvement

Though vendors are giving support in implementation and/maintenance but most of them are shopkeepers who employee semi-skilled technical workers. Institutes must take services of large consulting firms or consultants on periodic basis as these are certified professional people and adhering to their advice will certainly reduce security risks and performance of network will definitely improve.

It has been found that quite a number of institutions are using a mix of Branded and Non-Branded computers (PCs and Servers). But it is not clear in what ratio this is. A further study can be beneficial in this regard. Further, no norms have been set by any statutory education regulatory body which makes it compulsory for institutions to have only branded computers. These bodies, in the interest of both institutions and students at large, must make this compulsory to have only branded computers.

Majority of Institutions has Wi-Fi network but there is a difference between majority and 100%. Students and teaching staff are frequently been found to be carrying laptops, smart phones and tablets in classes. During lecture sessions, the students can open websites and find out more what the teacher
is teaching. Responses from students regarding Internet through Wi-Fi network is not very satisfactory. They have highlighted various issues like presence of Wi-Fi network in only limited areas of the campus, very low internet bandwidth on Wi-Fi network, etc. In some institutions, the Management has not even provided Wi-Fi to students and is restricted to only Staff members and Management. A.I.C.T.E. and other statutory bodies need to make presence of Wi-Fi network necessary in Professional Higher technical Education Institutions and specify the areas where Wi-Fi devices be installed and also mandate the I.C.T. security that must be involved in it.

- Maintenance and Technical Support not been found to be 100% perfect. A.I.C.T.E. and other statutory bodies need to make it compulsory for all Higher Technical Education Institutions to have a minimum number of trained I.C.T. Support Staff who must carry at least a government recognized diploma in Computer stream and must also have an Industry certification from Cisco / linux, / Microsoft. Regular upgrade of their skills is also necessary like is practiced in industries. Also the number of I.C.T. support staff should be in ratio of computers. Current students can also be appointed on limited hours basis to work as support staff in labs like what is practiced in developed nations under EARN-AND-LEARN initiative.

- Licensed Academic software are available in institutions but some students specially from computer and engineering faculties want to study and practice on these software at home. Student versions of these software can be made available to such students.

- Respondents have opinioned for Increase in Internet bandwidth. Government should subsidize the Internet bandwidth rates for educational institutions especially the higher technical education ones. Internet bandwidth can be increased but monthly quota of upload and download can be fixed per user basis. This will decrease wastage of internet data by users.

- Mild and High intensity I.C.T. security attacks are less frequent but are not completely absent. Low intensity attacks are more frequent than the former ones. Relevant security tools and equipment need to be used from now
itself so avoid turning low intensity attacks into high ones. User awareness
needs to be increased. Also, User awareness regarding Cyber laws and
relevant punishments under them need to be done. I.C.T. Security policy
also need to be made compulsory in each institute. Unified Threat
Management devise can be made compulsory in each institute.

- I.C.T. budget needs to be set. A.I.C.T.E. and other educational regulatory
  bodies can set I.C.T. budget in ratio of student enrolment. To make sure
  that this amount is actually spent, a compliance report submission may be
  made compulsory.

- I.C.T. security is not only the responsibility of service providers but also
  the users. Stringent penalties can be levied on both Staff and students if
  negligence is found from their side.

III) A theoretical model to improve efficiency of I.C.T. in Institutions imparting
Higher Technical Education: I.C.T.-Higher Educational Information
Security (I.C.T.-HEIS) Framework

After studying the conclusions, the researcher has put forward a framework titled The
I.C.T.-Higher Educational Infrastructure Security (HEIS) framework. This I.C.T.-
HEIS framework has been designed with the objectives to providing Data governance,
manage security issues, and aims at maintaining business continuity and build
competitive advantage in the Professional higher technical Education Institutions.
Figure: 5.1: I.C.T.-Higher Educational Information Security (I.C.T.-HEIS) Framework
This framework comprises 3 important components namely:

A) **The Institutional Functionalities:** Every higher technical education institution has certain aims and objective for which it has been established. These higher education aims and objectives are inculcated in very core on the institution’s existence.

1. These include
2. Research & Development
3. Digital content development
4. Teaching and learning (including e-Learning)
5. Curriculum
6. Assessment
7. Learning objectives
8. Industry-institute relationship
9. I.C.T. enabled learning equipment
10. Investment
11. Open education

Most of these objectives are associated with data that needs to be secured and has to be made available to right person at the right time using properly managed data e-governance. Much of this data is confidential e.g. exam papers, student academic records, research documentation, etc.

B) **The I.C.T. security architecture framework:** This encompasses the core I.C.T. security functionality. It is composed of 7 layers arranged in a logical manner. Each of these layers provides a certain level of functionality w.r.t. I.C.T. security. The next layer provides remedies in case there is a problem with the current level of security provided.

1. **Layer 1: I.C.T.-Enabled security layer:** This is layer provides the physical and logical security. Strategic security decisions are taken. The
heads of institution along with Technical Staff, carve out the I.C.T. security policies. The effectively use the IT Security Standards IT guidelines and procedures while staying in the bounds of IT Acts of the land. IT governance coupled with data governance is incorporated as per the policies formulated. I.C.T. security controls like firewalls, access lists, routers, antivirus, etc. help in providing I.C.T. security in physical form. A brief description of these terms is given below:

a. IT security policy- administrative and technical security
b. IT security standards- guidelines, procedures and best practices ISO, FIZMA, GLEBA etc.
c. IT controls: Management, technical, and operational controls
d. IT Acts: legal recognition for electronic communication
e. IT Frameworks and infrastructure: COBIT, ITIL, CMM, 6-sigma

2. **Layer 2: Risk assessment and analysis:** Though utmost care and effort is made in layer 1 to negate the possibility of I.C.T. security attacks, still no solution is 100% failure proof. The Risk assessment and analysis layer identifies and accesses the types of risk coming by various ways and their impact on higher educational infrastructure in terms of security.

This layer includes the following sub processes:

a. **Threats identification:** The threats to security may include one or more of the following: Virus, Hacking, Spyware, Natural Calamities, Rootkit, Backdoor attacks, threats from internal sources, etc.

b. **Vulnerabilities identification:** These are the open areas or exposed areas which could invite or transform into Threats. These may include poor network design, poor passwords, poor server and firewall configurations to name a few.

c. **Risk identification:** Here we identify the risks or damages that could happen in case the threats and vulnerabilities transform into a real I.C.T. security attack. Risks associated with I.C.T. security attacks on Higher Technical Education institutions include one or more of the
following: Cyber defamation, spoofing, economic crimes, IPR infringement

d. **Impact analysis:** This sub-process involves the analysis of level of damage which could be the outcome of I.C.T. security attack. The impacts may include financial impact, impact on goodwill, physical impact, privacy impact.

Impact analysis can be carried on 3 Levels. (i) low level analysis, (ii) mid-level analysis, and (iii) high middle analysis.

e. **Operational governance analysis:** Here analysis is done to find the overall impact on the business of the institution. Main analysis is about finding the impact of I.C.T. security attack on overall operational governance of the institution.

3. **Layer 3: Risk Mitigation initiatives:** To moderate the immediate effects of I.C.T. security attacks, at this stages, we design and install appropriate security controls at right place so that C-I-Aof educational infrastructure is achieved. These are the standard procedures or immediate steps to reduce the effect of an I.C.T. attack which need to be followed in case an I.C.T. security attack ever happens. It includes:

   a. **BCP (Business Continuity Plan):** to ensure that business runs during and post-disaster.

   b. **Security advisor:** to work as consultant in identifying the exact source of attack and propose immediate remedy to control the attack.

   c. **Access audit:** user access audit to find any deviations which transformed threats and vulnerabilities into actual security attack.

   d. **Access control:** immediate review of authentication-authorization-accounting to find vulnerabilities and take necessary changes.

   e. **Compliance:** government and regulatory bodies may give certain norms to comply to mitigate risks. Institutions need to comply to them.
4. **Layer 4: Solution Design:** After holistic analysis of threats, risks and suggested control, following solution is designed and is expected to the practiced by the institution so that similar I.C.T. security compromise doesn’t happen.

   a. **DRP (Disaster Recovery Plan):** This is one very important document. This document states how to recover from the aftermath of the security attack. This document provides various remedies to bring the institution and its business processes back on track. This document states the recovery steps in very specific terms and identifies the milestones that need to be attained in time-bound manner.

   b. **Asset classification:** based upon impact analysis, need to categories assets according to their criticality. This could be Low Critical assets, Mid-level Critical asset, Highly critical asset.

   c. **SLA (Service Level Agreement):** For the continuity of business processes, the I.C.T. infrastructure should have a minimum uptime guarantee. Certain aspects of I.C.T. infrastructure can be managed by the institution using internal sources but others need 3rd party support. When considering SLA one must consider the Asset Classification of the assets. Outsourcing the maintenance by Entering into AMC contracts and Service Level Agreements with Service centers, etc. provides Service continuity with established service design, service delivery, service support round the clock.

   d. **Evidence collection:** There needs to be a mechanism in place to look for evidence of I.C.T. security breach round the clock. Physical analysis of premises, log records of servers, etc. and employing Intrusion Detection Systems provide mechanism of collecting evidence of occurrence of I.C.T. security breach.

   e. **Communication:** There needs to be a communication system in place which is capable of communicating the occurrence of I.C.T. security attack or creation of possible vulnerability which could lead to I.C.T. security attack. This mechanism should also be able to communicate
the remedies to the users, support staff and administrators of I.C.T.
along with an effective feedback system to understand the
effectiveness of steps taken to counter I.C.T. attacks.

5. **Layer 5: Operationalize and enforce solution:** This layer is involved in
actual implementation of solutions which have been devised at layer 4.

a. **Testing:** The first part of this step involves testing of the proposed
design solution. This involves the implementation of solution for
testing purpose in either of the 2 ways: (i) Small scale implementation
of proposed solutions in a step-to-step manner. This involves
Implement—Wait-and-watch--- Proceed mechanism. (ii) Test the
solution in laboratory environment or test equipment to find the
possible outcomes. This gives time to I.C.T. administrators to ensure
that proposed solutions give a positive results.

b. **Training:** Before the solution is made operational, trained manpower
is needed to implement it and then work on it on day-to-day basis.
Training programs and Training Manuals need to be prepared. These
must be accompanied with user manuals.

c. **Awareness:** Awareness regarding the existence of the solution need to
be created among the stakeholders and users. Awareness creation can
be made by way of User interaction programs, monthly student
magazines, etc.

d. **Certification:** Users / administrators can be made to undergo
specialized vendor trainings and certifications like Microsoft
certification, Cisco certification, etc. This will ensure that the solution
is in professional hands.

e. **Accreditation:** Institution needs to go-in for accreditations like NBA
(academic), and other I.C.T. security related accreditations like ……

f. **ISMS (Information Security Management System):** Here the
framework uses the Information Security Management System which
is the ISO 27001:2005 international standard of best practices in the
field of establishing, maintaining, and improving security programs in
organizations and uses integrated processes to manage the administration of security program policies and procedures.

As part of ISMS, the educational institution needs to continuously review its security and constantly improve it. It required that all I.C.T. security related activities are recorded and there is periodic audit of these activities. To increase awareness about best practices, the institution is required to conduct training and awareness programs w.r.t. best practices needed under security management and its compliance.

6. **Layer 6: Maintain and improve infrastructure security:** Once the solutions have been operationalized, it is important that continuous maintenance and improvement is taken. For this purpose following steps need be incorporated:

   a. **Corrective & preventive action:** For the success of any system, it is important to analyze the performance of the system and if negative deviations in performance are found then corrective actions are needed to rectify the system. Preventive actions are needed to prevent any security hazards in future.

   b. **Responsiveness:** First of all the System should be so robust that no security attacks ever effects it. But if even there is a compromise in the security then response to such attacks should be quick and effective to minimize losses, destruction and down-time.

   c. **Audit:** There should be frequent internal and external security audits. These help in timely identification of prescribed procedures and finding security breaches which might have gone un-noticed.

   d. **Review:** After a few days of operation of the system, periodic reviews should be conducted. In this phase, audit reports should be studies, various failure reports must be examined. Apart from this, feedback should be taken from I.C.T. administrators on the operation and maintenance aspect. Feedback should also be taken from users and other stakeholders.
e. **Compliance Management:** It is beneficial for institutions to go in for standardization certifications like ISO. Other voluntary compliances could be NBA, NAAC, etc. while mandatory compliance include UGC, A.I.C.T.E., DTE and Affiliating university compliances. International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) are some of the international standardization organizations for I.C.T..

Being compliant to such compliance standards provides feedback on system operations and reduces vulnerabilities in the system.

f. **Enterprise Access Control:** Enterprise Access Control must be implemented across the institution. Access Right must implemented and duly audited. All users and employees of the institution should not have the same access level. Monitor real-time access logs and dashboards to see who accesses the network, when and what.

C) **The final Outcome:** If the Framework is properly and successfully implemented in the I.C.T. system, the institution gets the following TRIADS:

**TRIAD 1: Confidentiality-Integrity-Availability**

a. **Confidentiality:** The framework provides data governance through which limits access to information.

b. **Integrity:** As the data is secured and the framework is able to guarantee that the information is trustworthy and accurate.

c. **Availability:** Framework assures reliable access to the information by authorized people 24*7.

**TRIAD 2: Accuracy-Utility-Authenticity**

a. **Accuracy:** The Framework assures that the data values stored are the correct values and thus assures data quality.

b. **Utility:** The framework aims at timely delivering complete and accurate referenced data. This data is not only for running routine processes of the
institute but also involves data for use in critical regulatory reporting, transaction processing and risk management. At the same time it minimizes un-necessary costs for the institutions in terms of time and money.

c. **Authenticity:** framework provides authenticity to the data. It ensures that the data source is correct and what it claims to be or what it is claimed to be.

**TRIAD 3: Reliability-Portability-Efficiency**

a. **Reliability:** Framework ensures that data are reasonably complete and accurate. Framework ensures that data is checked at the time of input / import itself.

b. **Portability:** The framework strives to create I.C.T. infrastructure especially the databases and software (e.g. ERP) in such a way that it is easy to move, copy or transfer data easily from one database, storage or IT environment to another.

c. **Efficiency:** The framework ensures that there is efficiency in storage, access, filtering, sharing, etc. of data while not compromising with the transparency to the user. Managing storage growth, increasing amount of usable storage, and reducing overall storage costs is at the core of the framework’s objectives.

**TRIAD 4: Maintainability—Modularity-Testability:**

a. **Maintainability:** The framework strives to create a high probability of repairing a failed component or system or software or any part of the institute’s I.C.T. infrastructure. It ensures that it is restored or repaired to a specified condition within a specific period of time.

b. **Modularity:** The framework ensures that the software used in the institutions (especially the ERP systems) are modularized and inter-relation of the parts of a software package is smooth. Also, modularity in other aspects of I.C.T. infrastructure assures that all pieces of the I.C.T. infrastructure except the affected ones remain functional.
c. **Testability**: Testability is a way of conducting trials of the system and its various components. It determines and guarantees the quality and genuineness of the I.C.T. infrastructure.

**TRIAD 5: Completeness-operability-simplicity**

a. **Completeness**: The framework offers availability of all relevant data necessary to meet the current and future information demand. It proposes inclusion of data validation processes so that at the time of input of data itself, the complete data is stored.

b. **Operability**: The framework strives to provide mechanism that ensures that data is stored in such a manner that it can be later used directly, without additional processing: restructuring, conversion, etc. The software that are going to be used in the institutions will store data in most common formats like SQL and XML which can be easy be read by other software.

c. **Simplicity**: To maintain simplicity of data, the institutions data collection sources will be narrowed down so that the complex processes for gathering data and turning it into meaningful information become simpler. The framework aims at cutting down the extra steps involved in data collection and processing.

**5.4 LIMITATION OF THE STUDY:**

This research study, like other research studies has certain limitations. Some of these are:

- It covers geographical area Pune which is quite industrially and academically developed. Findings could have been different in case of smaller cities.

- Certain deeper technical aspects of PCs and Servers have not been covered as the study is more Management oriented.

- Medical institutions and simple Undergraduate courses like BA, B.Com, etc colleges have not been covered.

- University which is the highest body for imparting higher education has not been individually studied.
5.5 FURTHER STUDY:

The Researcher wanted to conduct a deeper study on the I.C.T. infrastructure and its security but due to time constraint this was not possible. Thus, this study has left open certain areas for research and created new ones which researcher would like to himself undertake as post-doctoral research or they can be used by researchers in future. Some of these areas are:

- Study of I.C.T. infrastructure in agricultural educational institutions located in Rural areas.
- Study of I.C.T. infrastructure in Diploma-level educational institutions located.
- A study of I.C.T. security audit system in educational institutions
- A study of I.C.T. infrastructure in schools / graduate level colleges in tier-2 cities.

5.6 CONTRIBUTION OF RESEARCH TO EXISTING BODY OF KNOWLEDGE

The suggestions will give clear cut guidelines for managing the implementation and maintenance of I.C.T. which will become the baseline for the higher technical education facilitators in the country.

Government has made many policies relevant to this area of study but have some problems at implementation level, these have been pointed out and remedies have been suggested in the study.

SUMMARY:

In this chapter the researcher has described various finding which the researcher has observed after analyzing the data collected. Relevant conclusions have been arrived upon and based on these the researcher suggested certain solutions.