**Operating system**

**Stid:59290**

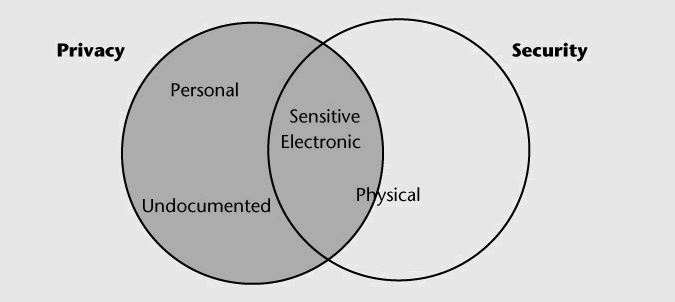
**Name : rameez**

**Introduction:**

Computer security now a days it is very necessary to improve the lebel os security in you,r computer system the secure system would always be prefer over a fast and well developed ssytemthere are some techniqal issue which we need to face now a days in computer security system the hot topic now a dys is how to secure you,r digital system millatry system is quite secure and asvance their data is afe and we can also take motivation from them in securing out whole system

Once the computer system begins its work for a useThe relation of privacy and security as we see below in figure we are trying to elaborate here that if we see on the privacy side we must focus on that “what, who and where” our documented or undocumented data concerned from, but on the security side our vision is to put a light on how our data to be committed with the systems rather our securing techniques which we used can be on physical side of our systems

r, security is facilitated at three levels: the hardware level, the software level, and the data level. In addition, if the computer system consists of terminals or several computers, then intercommunications between terminals and computers and among computers require security considerations



To be practical, the defense mechanism must work transparently with third-party software whose source code may not be available. Our binary rewriting tools analyze binaries and add system call location information to them, without requiring the source code. This information is contained in a new section of an ELF binary file. Our modified OS kernel checks system call addresses only if an executable contains this additional section. This makes our approach flexible: if an executable does not contain this section, the intrusion detection mechanism is not invoked. It is therefore possible to run unmodified third-party software as-is, while at the same time protecting desired executables; the use of binary rewriting means that an executable can be protected without requiring access to its source code