**INTRODUCTION**

The term ”mobile computing” refers to a set of technologies that create a setting in which users can share any kind of data with other devices that aren’t physically attached to one another [1] To put it simply, the data can be sent from anywhere in the world via wireless transmission. There are three pre- requisites for effective mobile computing. They let users to create connections, and they comprise both the hardware and software of mobile devices. The protocols, services, and other aspects that make up the mobile communication framework ensure that communication flows without any hiccups. The hardware devices used in mobile computing can be taken anywhere and remain linked to the internet, which is the main driving force behind the success of this technology[2]. Beginning with the development of the first laptops in the 1980s, the era of mobile computing was born. Fast forward to 1990, and we have Apple’s 640\*640 portable computers, made possible bya number of upgrades and changes to the original hardware. It continued with the introduction of the first personal digital assistant (PDA) in 1993 and the first smartphone by IBM in 1994. Connectivity to networks was enabled in smartphones in the 2000s, the first iPhone debuted the following year, and the first Android smartphone was developed the same year. There is a wide range of mobile computing devices available now, each with its own set of features that expands with each new version of the underlying hardware and software[3-5].

As the number of features increases the number of users using these mobile computing devices rises tremendously In 2022, there will be more than six billion smartphone subscriptions globally, and Statista predicts that this number will expand by several hundred million in the next years, with the largest increases expected in China, India, and the United States[6]. Mobile phones are not only been used for communica-tion purposes, but It has also expanded their usage of capacity.Nowadays mobile phones are being used as personal assistants. They are being used for calls, payments, online shopping, gathering information, social media, booking appointments, ordering stuff, etc. With the rise in the tremendous growthof technology on one side, it raises serious questions about security[7,8]. The security factor is equally important to both the service provider end as well as endpoint side. When it comes to security it must be given to all the phases like in hardware part, software part, and network part. Hardware security islike protecting the physical machine from threats and attacks. Software security is something that gives protection to the software by providing integrity, authentication, and availabil- ity. Whereas network security is providing security to thenetwork, the medium. When data is let to transmit to another device through the network, it is more prone to be insecure. The major concern in security is to provide confidentiality, integrity, and availability of data. Information is an asset toall. it cannot be left as it is in a network because anyone using the network can view them. Network security has becomea major concern in the scope of security. A secure data transfer is transferring data from one place to somewhere with the assurance that the data is confidential, not modified or intercepted during transit. So, when the data is transmitted, it should be transmitted in a secure way over a secure channel. There are many ways to secure transmission. We can use various cryptographic techniques, steganographic techniques, firewalls, access control, and Intrusion Detection Systems to protect the data.

|  |
| --- |
|  |
|  |  |