Many researches in the past ignore the need to encrypt the data for security perspective. However in recent years, researchers have given top priority for data security for smooth transmission of data over network by incorporating many encryption strategies along with actual data. In this paper, we consciously discuss the need to secure the data for patient monitoring using various algorithms and plug out the one which is best suit for inbound data security for future healthcare application. As the fields of IoT and Cloud are distinct by their intrinsic technologies, there is a need for integration of Cloud with IoT is obligatory to facilitate and resolve issues involved in data storage as well as data security. In the field of modern healthcare environment, automation has emerged to be more necessary to route and stock the facts about employers (doctors), employees (staffs) and customer (patients). Hence doctors in need of such a stored voluminous information’s about a particular person, whom which the condition has to be diagnosed. The clinical and other facts about a person is indeed to be private (trust worthy) and should not be revealed by any other private identity. While establishing bi-directional connections to the internet, communication is a threat and has to be
secured without involving any security threads. The offered work makes use of blow fish data encryption and IPv6 based addressing scheme for high data security and increased probability of number of nodes to reduce network congestion.

References


Index Terms

Computer Science

Security

Keywords

Encryption, inbound data security, automation, network congestion, addressing scheme