SECURITY IN IoT BASED HEALTHCARE SYSTEMS

Online diagnosis is a widely used standard data service in current healthcare systems. Real-time physical data is collected with the help of IoT via body sensors and software, which informs real-time decision-making with the help of online diagnosis. As the collected user data and diagnosis results contain sensitive information, a privacy leakage or hacking might lead to misguidance or even fatal incidents. As a third-party cloud service is involved, data protection is becoming a serious issue. On the other hand, with resource constrained IoT devices, standard security measures are not provided. Regarding the parameters, less computation time with low cost, proper steps for anonymity, adaptability and accuracy should be considered. To overcome these shortcomings, designing a lightweight algorithm providing both high security and less computation time is needed. Also, the implementation of AI for both data processing and assisting online diagnosis is to be done.

CURRENT STATUS –

1. A third party provides cloud platforms to the cloud client, data protection is the primary issue.
2. Standard security (counter) measures are not effective, with the presence of resource constrained IoT devices.
3. Centralized database - security problems Denial of Service (DoS) attacks and a single point of failure.
4. the collected user data, diagnosis results and the deployed machine learning model contain sensitive information of users and the healthcare provider, which may lead to serious privacy leakage.

LIMITATIONS IN CURRENT SYSTEM

1. Computation time
2. High cost
3. No measures for anonymity
4. Centralized systems
5. Security from third party cloud.
6. Adaptability for moving IoT devices

EXISTING ALGORITHMS

1. Elliptic Curve Cryptosystems (ECC)
2. Advanced Encryption Standard (AES)
3. Data Encryption Standard (DES)
4. BlowFish

PROPOSED WORK

This study proposes the design and implementation of a robust three-tier architecture utilizing blockchain technology for the purpose of ensuring the secure storage of patients' health data. The architectural design will incorporate blockchain technology in order to guarantee the integrity of data records and improve the interoperability of the system. By keeping an eye on and tracking all events connected to database data, this will be possible.

Develop a robust algorithm, based on blockchain technology, that ensures secure access to health records. This study aims to investigate the possible application of blockchain, a decentralized and distributed technology, to mitigating security challenges inside Internet of Things (IoT) networks enabled by 5G technology. This study aims to propose a pragmatic framework for the integration of blockchain technology in order to enhance the security of cellular-enabled Internet of Things (IoT) networks, with a particular focus on the principle of decentralization. The proposed model utilizes a hybrid self-clustering evolutionary algorithm (EC) that integrates genetic algorithms (GA) and simulated annealing (SA) techniques. This approach aims to effectively divide the Internet of Things (IoT) network into distinct clusters, thereby improving its multi-layer architecture and prolonging the network's longevity.