**Research Topic: Enhancement of Healthcare Security through Machine Learning Innovations:**

**Related Article -03**

1. **Problem Statement:** The integration of the Internet of Things (IoT) with healthcare, also known as the Internet of Medical Things (IoMT), allows for remote patient monitoring and diagnosis. However, IoMT poses substantial security and privacy risks, particularly given the sensitive nature of medical data, the vulnerability of medical devices to cyber-attacks, and the limitations of standard security solutions.
2. **Proposed Solution:** The research suggests applying machine learning (ML) techniques to improve the security of IoMT devices and healthcare systems. ML techniques are specifically recommended for anomaly detection, intrusion detection, authentication, and defense against a variety of assaults, including poisoning and Trojan attacks.
3. **Technical Implementation:** The proposed solution involves combining ML techniques with IoMT infrastructure. Various ML techniques, including as supervised, unsupervised, and deep learning, are used to detect anomalies, unauthorized access, and intrusions. Furthermore, cryptographic techniques such as homomorphic encryption are employed to protect sensitive medical data during transmission and storage.
4. **Experimental Setup:** Medical data from IoMT devices is used to train a variety of ML models, including Artificial Neural Networks (ANN), Decision Trees (DT), Support Vector Machines (SVM), and Random Forest (RF). The models are utilized for tasks like medical sensor anomaly detection and authentication. Datasets are tested to determine performance in real-time IoMT settings.
5. **Results:** ML techniques, particularly ANN, DT, and RF, are highly accurate in anomaly detection, with detection rates of more than 99%. Furthermore, the adoption of encryption technologies protects data privacy and security in IoMT networks. The use of ML and encryption substantially reduces security threats in healthcare settings.
6. **Comparison:** In comparison to traditional security approaches, ML-based systems detect attacks and anomalies faster and more accurately in real time. Traditional systems struggle with the limited resources of IoMT devices, whereas ML models can adapt and improve in real time. Furthermore, homomorphic encryption enables secure data transmission by eliminating the need to decrypt sensitive data.
7. **Limitations:** One of the most significant drawbacks is the computational burden associated with deploying ML models on resource-constrained IoMT devices. Furthermore, some ML-based assaults, such as poisoning and Trojan attacks, have the potential to modify training data, compromising model accuracy. Fully homomorphic encryption is also resource-intensive and may not be suitable for all IoMT applications.
8. **Future Work:** The research recommends looking into new lightweight encryption approaches and enhancing ML algorithms to reduce computational requirements. It also suggests more research into detecting and blocking advanced ML-based assaults, such as model poisoning and neural trojans.
9. **Contributions:** The study presents a comprehensive strategy to safeguarding IoMT systems that employs machine learning and encryption. It emphasizes the significance of real-time anomaly detection and safe data transfer in healthcare, providing practical solutions for privacy and security in IoMT-based healthcare systems.
10. **Applications:** The proposed solutions are applicable in a variety of healthcare situations including remote patient monitoring, real-time diagnosis, and secure medical data storage. They are especially beneficial in situations where IoMT devices acquire sensitive health information, such as hospitals, clinics, and home healthcare settings.

**Related Article -04**

** Problem Statement:** As healthcare systems become more digital, they confront greater cyber dangers. The integration of connected medical equipment, electronic health records, and telemedicine has exposed healthcare systems to new security risks that may jeopardize patient data and services.

** Proposed Solution:** The paper representatives securing healthcare systems with sophisticated technologies such as block chain, artificial intelligence (AI), and the Internet of Things (IoT). These technologies provide safe data storage, threat detection, and real-time patient monitoring, which can help guard against cyber-attacks.

** Technical Implementation:**

• Block chain technology ensures secure and tamper-proof sharing of patient data.   
• AI identifies security concerns in healthcare data by detecting unexpected patterns.  
• IoT connects medical devices to monitor patients in real-time, but requires strong security measures to avoid data breaches.

** Experimental Setup:** The article discusses several real-world examples of how these technologies have been successfully utilized in healthcare settings. AI, for example, is used to detect threats early on, and blockchain safeguards medical records' integrity.

** Results:** These technologies have enhanced healthcare system security by securing sensitive patient information, swiftly detecting security threats, and allowing for secure remote patient care.

** Comparison:** Blockchain is more safe against data manipulation than traditional security methods; AI detects threats faster and more accurately; and IoT delivers better patient monitoring but requires more robust security to manage sensitive data.

** Limitations:** Privacy concerns, regulatory compliance, and integration with existing healthcare systems are among the challenges. Because of their networked nature, IoT devices are especially sensitive to security threats.

** Future Work:** Future initiatives will center on developing strong ethical and regulatory frameworks, improving technology interoperability, and training healthcare personnel to utilize these technologies successfully. There is also a need to give patients the ability to handle their own data securely.

** Contributions:** The article demonstrates how combining blockchain, AI, and IoT may greatly improve healthcare system security, ensuring data confidentiality and better patient care.

** Applications:** These technologies improve healthcare safety and efficiency by enabling secure patient data management, remote monitoring, and early identification of security threats.