Name: Sadia Akter
Id: 2125051059
Sec: 7B1

Assignment 3:

Task 01: According to your related topics, read two survey or review paper as well as extract information and fill-up the table.

Solution:

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

TABLE: 01

Ref.	Problem area	Data type	Data size	Data Sources	Availability
[1]	**Security and robustness of ML models in healthcare applications**	EHRs, medical images, clinical notes	Varies by task (e.g., medical image datasets, clinical data)	Healthcare institutions, open Medical repositories (MIMIC-III, etc.)	Public and proprietary datasets
[2]	**Healthcare IoT security, data protection, and privacy**	Sensor data, IoT data streams, health monitoring signals	Billions of IoT devices by 2025	IoT sensor networks, wearable devices	Limited due to privacy concerns; data shared through secured frameworks

Here Are The Related Topic References:

1. [1] - "Secure and Robust Machine Learning for Healthcare: A Survey"
2. [2] - "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation"

TABLE: 02

Ref.	Methods/ Techniques	Results/ Outcomes	Research gap/ Limitations	Future Directions/ Future work	Opinion/ Comments/ Feedback
[1]	- Adversarial ML defense techniques - Privacy preserving ML - Secure data pipelines - Model robustness strategies	- Showcases effectiveness of ML for diagnostics and prognosis - Improved model accuracy but security remains an issue	- Lack of real-world testing for adversarial defenses - Data privacy challenges in clinical use cases	- Further work needed in privacy preserving ML and secure model deployment in healthcare environments	- The study emphasizes the need for collaboration between healthcare providers and tech researchers
[2]	- IoT-based anomaly detection - Machine learning for intrusion detection - Secure communication protocols for IoT devices	- ML improves the detection of cyber security threats in IoT environments - Enhanced real time monitoring capabilities	- Limited availability of IoT-specific healthcare datasets - Lack of standardized security protocols across devices	- Explore integration of 5G with IoT for real time, large-scale healthcare applications	- Effective for IoT security, but requires more robust data sharing frameworks to ensure patient privacy