CYBER ATTACK DETECTION AND PREVENTION SYSTEM OPTIMIZED STACKED RECURRENT NEURAL NETWORK

A PROJECT REPORT

Submitted by

SRI MUTHU CHARUVAGAN M
VEERA VIKAS S
YOUSUF AKTHAR K M

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

PSNA COLLEGE OF ENGINEERING AND TECHNOLOGY,
(An Autonomous Institution Affiliated to Anna University, Chennai)

DINDIGUL - 624622

MAY 2024

ABSTRACT

The domain of cybersecurity encompasses various areas such as network security, information security, application security, and more. An existing problem within cybersecurity is the increasing sophistication of cyber threats, including malware, ransomware, phishing attacks, and insider threats, which pose significant risks to individuals, organizations, and governments worldwide.

Cyber attacks can result in data breaches, financial losses, reputation damage, and even physical harm in some cases. They disrupt operations, erode trust, and can lead to legal repercussions. Additionally, they often require significant resources to mitigate and recover from, impacting both organizations and individuals alike.

Recurrent neural networks (RNNs) are adept at analyzing sequential data, making them invaluable for cybersecurity. By learning patterns from historical data, RNNs excel in anomaly detection, flagging deviations from normal network or system behavior that could signal an attack. They enhance intrusion detection by recognizing suspicious activities or known attack patterns in real-time, enabling swift response to threats. RNNs also aid in predictive analysis, forecasting potential cyber threats based on past incidents. Furthermore, they excel in malware detection by scrutinizing software behavior for signs of malicious activity.