



BANKING PROTECTION & THREAT DETECTION MODEL

MODY UNIVERSITY OF SCIENCE & TECHNOLOGY

OVERVIEW

Cybersecurity in banking and finance is a vital practice aimed at safeguarding financial institutions and their customers from cyber threats and attacks. This sector is a prime target due to the valuable financial data it manages. Key aspects include data protection, strong authentication, network and application security, phishing prevention, incident response planning, compliance with regulations, threat intelligence, and security awareness programs. With the rise of remote work and cloud services, securing remote access and cloud data has become increasingly important. Regular testing, monitoring, and a proactive stance against cyber threats are essential to maintain the integrity, confidentiality, and availability of financial data and services.



CONCEPT

01

CLIENTS

02

DESIGN

03

BUILD

The target of our model are banking and financial clients looking for relief from cyber threats and attacks.

Python is used in this model to design it for strengthening the security and detecting any real time threats and to give quick response.

Python libraries like pandas and numpy are used to build this AI/ML model, which is trained with ample amount of data to make it work smoother.

FUNCTIONALITY

The code provided, defines a AI/ML model that is trained by gathering data from various sources within the banking and financial environment and processing it until it identifies patterns and anomalies. It alert system to trigger notification when threats or anomalies are detected. Incident response procedure are initiated automatically or by cyber security experts to mitigate threats. It also conduct regular scan and assessments to identify volunariblity in systems and applications.

OUTCOME

IMPROVED CYBERSECURITY RESILIENCE

Strengthens overall cybersecurity defenses of banking and finance institutions.

PROACTIVE THREAT DETECTION

The proactive approach helps prevent successful cyberattacks before they occur

REDUCED RESPONSE TIME

The swift response minimizes potential financial and reputational damage caused by cyberattacks.

ADAPTATION TO EVOLVING THREATS

The system is designed to adapt to evolving cyber threats and technologies, ensuring long-term cybersecurity resilience

THANK YOU!

TEAM MEMBERS:-

- YUBIKA SINGH
- RISHU CHOUDHARY