# Blockchain-Enabled Security Framework against Ransomware Attacks Using Machine Learning

## Aim:

Our study aims to introduce a Blockchain-Enabled Security Framework against Ransomware Attacks using Machine Learning to ensure high protection and prevention.

## Abstract:

RANSOMWARE is a type of malware attack in which the attacker encrypts and locks the victim's data and crucial files, and then demands money (ransom) in exchange for the data to be unlocked and decrypted. Cybercriminals utilise ransomware as a sort of malware (malicious software). If a ransomware attack happens on a device, it either limits access or encrypts the data (files) of the device. Cybercriminals demand ransom (some amount of money) from their victims in exchange for releasing the data (i.e., to provide the decryption key). A close eye and security software are recommended to protect against ransomware outbreak. Most of the organizations, such as financial institutes and healthcare sectors are targeted by ransomware attacks. Ransomware assaults are among the most frightening types of cyber-attacks, and they are not confined to a specific sector or the countries. Blockchain is a tamper-proof technology, which is more secure, robust and decentralized in nature. Features of blockchain can add more security for detection and mitigation of ransomware more effectively. The application of machine learning algorithms and techniques is to identify and recognize patterns, anomalies, or specific objects within data. In this paper, we propose a new blockchain-enabled security framework using machine learning to detect and defend the ransomware attacks.

## Existing System:

In the Existing System, they mainly focused only on the aftermath of ransomware attack by detection of ransomware and recovery of data. They didn't proposed how to prevent the system from the ransomware attack.

## Disadvantages:

The proposed system didn't focused on the antecedence of ransomware attack will continue to be a significant drawback.

## Proposing System:

In the proposed system, we focused on antecedence of ransomware attack as well as aftermath. We also provided a demo attack of Locker Ransomware and Crypto Ransomware to get real-time experience and to aware of it. We will also continuously monitor the system, if any suspicious files is detected it will be removed automatically. We will take backup of the user data to recover it later, in case of ransomware attack so that we don't need to pay ransom to the attacker. In detection on ransomware we will mainly focuses on the portable executable files which plays a major role in gaining access of the system. We will do the detection of ransomware in Portable Executable files using Honeypot dataset and then the features/signatures are extracted followed by Feature Selection, Correlation and Classification using Machine Learning to detect that the executable file is Legitimate or Infected.

## Advantages:

The continuous monitoring of the system and automatic removal of files, in the event of suspicious activity followed by detection of ransomware and recovery of data make this proposal to stand out than the others.

User:

User will login to their account to take back-up of their resources in blockchain, In order to retrieve their data in case of ransomware attack. User can scan their files to know that the files are infected or not. At the worstcase, if are’nt no chances to recover their data after the attack they can pay the ransom securely through blockchain to the attacker.

Attacker:

Attacker show the demo of Locker Ransomware and Crypto Ransomware from their Login. Attacker also receives ransom after ransomware attack from the victim in exchange for restoring access to their data.

Detection of Ransomware using Machine Learning:

In our proposed system, Machine Learning will play a vital role in the detection of malware portable executable files. The user will scan the executable files using react user interface and then features from the files are extracted followed by Feature Selection, Correlation and Classification using Machine Learning to detect that the executable file is Legitimate or Infected. To achieve this, the suitable dataset will be downloaded and data pre-processing will be done to remove outliers and to check if there are any null values. After data pre-processing, feature selection will be done using variance threshold to select the most important features followed by correlation to remove the highly correlated features. We will use the Lazy classifier algorithm to determine which algorithm gives better accuracy. Based on the result we will use the highly accurate classifier to detect the portable executable file is malware or legitimate.