Blockchain-and ML based Malware Detection and integrity checking : A Decentralized Approach

Aim

- malware and integrity checking of files in a decentralised way.

Malware detection problems

- Traditional malware detection systems rely on signature-based detection methods and pattern matching techniques to identify known malware threats. However, these methods have limitations that make them less effective in detecting new and unknown types of malwares, which are increasingly common in the real world.
- they can only detect known threats that have already been identified and added to a signature database. This means that if a new or modified malware variant is released, it may go undetected by traditional detection methods until it is added to the signature database.
- As well as There are several challenges in making generalized malware detection models. Malware is constantly evolving, with new variants and attack methods emerging regularly. This makes it challenging to build a generalized model that can detect all types of malwares.
- Adversarial attacks are techniques that are used to bypass or manipulate machine learning models. In the case of malware detection models, adversaries may use these attacks to evade detection.
- Malware detection models need to be fast and efficient, particularly when used in real-time environments. The computational overhead associated with some machine learning algorithms can make them impractical for use in some environments.

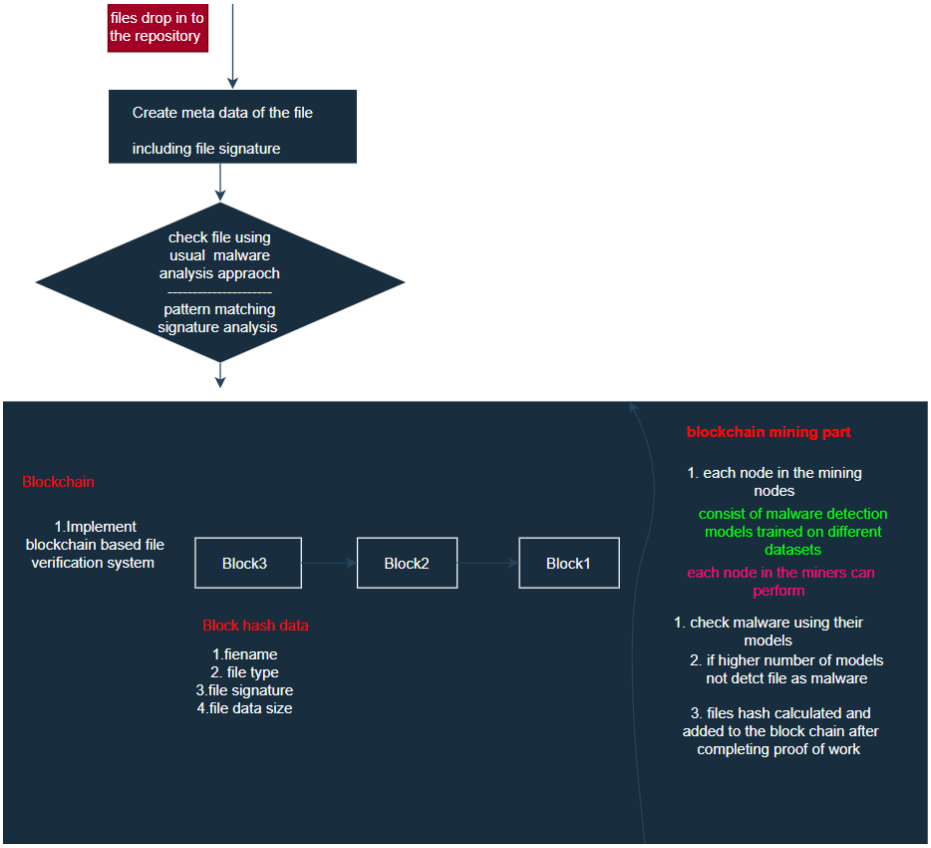
File integrity checking problems.

- Traditional file integrity checking methods rely on cryptographic hash functions to generate a unique digital fingerprint of the file, which can be used to verify the file's integrity. However, if an attacker can tamper with the file, they can also modify the hash value, making it difficult to detect the tampering.

Solution

- Multi model approach to detect malwares in organizational repositories.
- Blockchain technology can be used in file integrity checking to provide a tamper-proof and transparent record of a file's history.

Approach



- files are dropped into the repository and metadata is created for each file, including its signature. The files are then checked using traditional malware analysis methods such as pattern matching and signature analysis.

- The blockchain-based file verification system is implemented by creating a block hash data that includes the file name, type, signature, and data size.

- In the blockchain mining part, each node in the mining nodes is equipped with a malware detection model that has been trained on different datasets. When a new file is added to the repository, each node checks the file using their respective models. If a higher number of models do not detect the file as malware, the file's hash is calculated and added to the blockchain.

- Overall, this approach provides a decentralized and more secure way to detect and prevent malware attacks. By leveraging the power of blockchain technology, the system can ensure the integrity and authenticity of files, while also leveraging the knowledge and expertise of multiple nodes in the network to enhance malware detection capabilities.