|  |  |
| --- | --- |
| **TITLE OF THE PROJECT:** | BITCOIN HEIST RANSOMWARE ATTACK PREDICTION USING DATA SCIENCE PROCESS |
| **NAME OF THE STUDENTS:** | HARSHAVARTHINI R, ISABELLA MARY J, MUTHUPRIYA M |
| **REGISTER NUMBER(S):** | 211419104097, 211419104106, 211419104172 |
| **NAME OF THE GUIDE:** | Dr.T.Jackulin,M.E.,Ph.D.,  Associate Professor |

**ABSTRACT**

The cryptocurrencies, such as Bitcoin, are a form of digital currency designed to work outside of the traditional banking ecosystem. Cryptocurrency transactions, aka the buying and selling of digital currency, are typically handled using a crypto-exchange platform. These transactions often involve large sums of cryptocurrency, typically anonymized utilizing the blockchain, hence attracting cybercriminals. Proliferation of cryptocurrencies (e.g., Bitcoin) that allow pseudo-anonymous transactions, has made it easier for ransomware developers to demand ransom by encrypting sensitive user data. The recently revealed strikes of ransomware attacks have already resulted in significant economic losses and societal harm across different sectors, ranging from local governments to health care. However, although Bitcoin transactions are permanently recorded and publicly available, current approaches for detecting ransomware depend only on a couple of heuristics and/or tedious information gathering steps (e.g., running ransomware to collect ransomware related Bitcoin addresses). The proposed work undergoes four machine learning algorithms namely Logistic Regression, Random Forest Classifier, XG Boost Classifier and Voting Classifier among which XG Boost Classifier gives the maximum accuracy of 91.34%.