iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44629

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Crypto Currency Mining Farm for E-Vehicle using ML

Sharon Candeda Jones[1], Sumathi. N[2], Jeyakarthiga. R[3]
[1, 2, 3]*Electronics and Communication Engineering, Jeppiaar Engineering college, ANNA University: Chennai*

Abstract: ***Globally Travelling/ Transportation charge is getting to an extreme high due to the demand of non-renewable resources like Petrol & Diesel, Electronic Toll Collection and Vehicle Parking Expenses all leads to make the travelling cost unaffordable. In order to solve this problem, the automobile industry has proposed new ideas like Electric Vehicle which will replace the usage of existing high cost non-renewable resources like Petrol & Diesel, in the same way Automobile Industry proposes a new idea to reduce the Expenses of Electronic Toll Collection Charges, Vehicle Parking Expenses, and expenses like Electric Vehicle Charging Station Bills, In this proposed system hereafter all the next generation vehicles should come up with a new technology called Crypto Currency Mining Farm(CCMF) which will do Standalone Mining in the vehicle end and earn Crypto Currencies, This Crypto Currencies will be used for meeting all types of expenses for the Vehicle , it means Vehicle will earn Crypto Currencies and spend for all the listed expenses without disturbing the Vehicle owner which will make the cost affordable.***

I. INTRODUCTION

A. General

In the last few years, the mobile devices have become an extending support for various applications in areas like financial, medicine, science. This is because of the need for mobility and accessibility of mobile communications networks for many end-users acting in residential or corporate sites and performing various tasks according to their applications.

Within this general framework, one can see that Android is currently the most popular operating system for mobile devices. This trend is proven by the evolution of the market shares of Android OS (operating system) during the last years. Its fast adoption leads to an increasing rate of malware occurrences comparing to the previous years.

The increasing functional capabilities that Android platform provides to the various applications of the end-users become a source for new vulnerabilities and attack points that can be exploited the malware developers. In many cases, the malware spreading opportunity is supported by the third-party applications stores availability. This is because these third-party developer applications are typically hosted in Google Play.

The malwares for mobile devices (with Android OS) include viruses, Trojans, adware, backdoors, worms, botnets, spyware, ransom ware and other applications that are designed for malicious purposes using various implementation methods such as code obfuscation, dynamic execution, stealth techniques, encryption and repackaging.

In order to avoid the actual anti-malware mechanisms for Android the most applied techniques that are used to attack the Android platforms (devices, OS and installed applications) include sending messages without the target's awareness and deleting them by itself, fraudulent sending of user's private data.

The Android malware could also be classified based on their behavior, as following: Information extraction malware, Premium Rate Calls and SMS, Root Exploits, Search Engine Optimization, Dynamically Downloaded Code. According to the Malware bytes LABS report published in 2017, in 2016 ransom ware increased to the top, targeting especially business.

It is a cyber-criminality industry based on the new paradigm of Ransom ware as a Service (RaaS). During the last quarter of 2016, nearly 400 variants of ransom ware were identified. As concerning the specific Android malware, the Malware bytes LABS report shows that the most important trend in 2016 was the increasing use of randomization as an approach of the malware developers to bypass the detection mechanisms. The purpose of this research activity is to define a design methodology for an anti-malware solution addressing Android platforms, based on advanced machine learning techniques. The application goals are the detection and recognition of various malware having as their targets the mobile devices and apps. The modeling process should allow accurately recognizing and detecting the malicious apps before producing serious damages by compromising the end-user's sensitive data and their privacy.

The rest of the paper is structured as following. Section II presents related works about the most relevant developments in the area of anti-malware solutions while Section III proposes a methodological framework for design and development of Android malware detection solutions; Section IV draws conclusions and outlines further research lines in order to design, develop and implement optimized solutions taking in account the various real applications constraints

B. Crypto Currency

Crypto currency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, crypto currency payments exist purely as digital entries to an online database describing specific transactions. When you transfer crypto currency funds, the transactions are recorded in a public ledger. Crypto currency is stored in digital wallets. Crypto currency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting crypto currency data between wallets and to public ledgers. The aim of encryption is to provide security and safety. The first crypto currency was Bit coin, which was founded in 2009 and remains the best known today. Much of the interest in crypto currencies is to trade for profit, with speculators at times driving prices skyward.

Crypto currencies run on a distributed public ledger called crypto currencies, a record of all transactions updated and held by currency holders. Units of crypto currency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins. Users can also buy the currencies from brokers, then store and spend those using cryptographic wallets. Although Bit coin has been around since 2009, crypto currencies and applications of block chain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.

A crypto currency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many crypto currencies are decentralized networks based on crypto currencies technology a distributed ledger enforced by a disparate network of computers. A defining feature of crypto currencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation. A crypto currency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities. Experts believe that block chain and related technology will disrupt many industries, including finance and law. The advantages of crypto currencies include cheaper and faster money transfers and decentralized systems that do not collapse at a single point of failure. The disadvantages of crypto currencies include their price volatility, high energy consumption for mining activities, and use in criminal activities.

C. Block Chain

A block chain is a distributed database that is shared among the nodes of a computer network. As a database, a block chain stores information electronically in digital format. Block chains are best known for their crucial role in crypto currency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a block chain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

1) How to Secure the Block Chain

Block Chain is a type of shared database that differs from a typical database in the way that it stores information; block chains store data in blocks that are then linked together via cryptography. As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order. Different types of information can be stored on a crypto currencies, but the most common use so far has been as a ledger for transactions. In Bit coin's case, crypto currencies is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control. Decentralized crypto currencies are immutable, which means that the data entered is irreversible. For Bit coin, this means that transactions are permanently recorded and viewable to anyone. Figure 1.2 describes the crypto currency technology.

Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

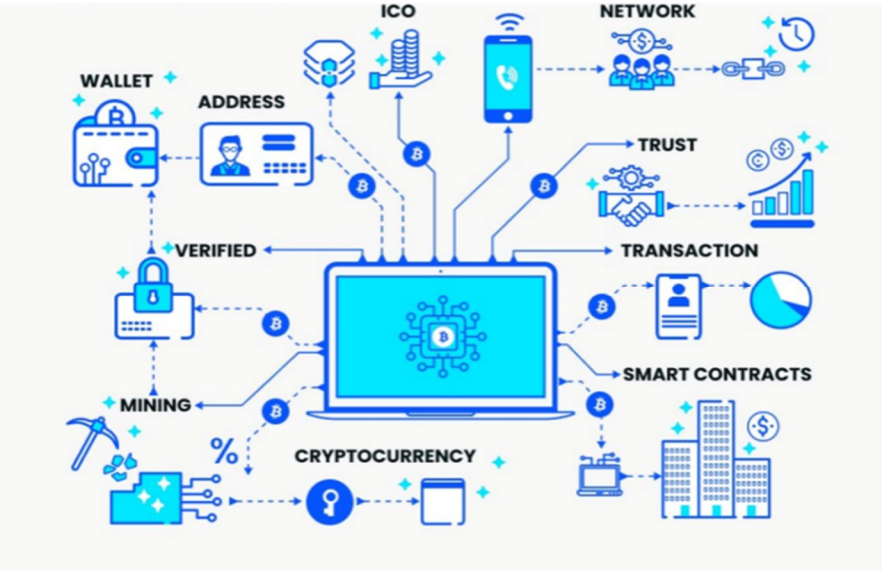


Figure 1.1 Crypto currencies Technology

D. Problem Statement

In this project work, we aim to create a webpage towards the ETC Tollgate side with respect to knowing the amount transaction within the date and time of respective event based on the amount debited from the wallet, Then the balance statistics and wallet balance with the graphical analysis can able to see from the created webpage. Keeping these points in view, thesis title is as under:

E. Objectives And Scope

The proposed work contains two modules 1. CCMF in the vehicle 2. toll collection, CCMF is a device can be installed by any low voltage. Which will convert electrical energy to digital money. Tensilica's 32bit processer is used in crypto currency mining farm. Crypto currency mining farm will connect with internet, inside the vehicle and access the crypto currencies and will start the mining process and will earn the Crypto Currency and moves the Crypto Currency to the Digital Wallets. This will be used for all expenses on the later stage and a Wi-Fi module is attached for the internet. Wi-Fi module with 2 relay is provided in the ETC side for toll gate access and EV charging. Once pay mode switch is pressed automatically the amount from the digital wallet from vehicle will transferred to the ETC as toll fee and something will be detected from the our digital wallet. The same process will be followed for all the expenses like Charging and parking.

1) To develop a CCMF device which is installed by a low-voltage and then to convert electrical energy to digital money in the vehicle.
2) To maintaining The CCMF will be connected with internet, inside the vehicle and this will access the crypto currencies, which will further start the mining process.
3) To earn the Crypto Currency and moves the Crypto Currency to the Digital Wallets.
4) To use Crypto Currencies for all types of expenses for the Vehicle. Such that the expenses will be like Toll collection charges, Parking charges and Electric vehicle charging station bills.

F. Organization Of The Report

The proposed work is arranged in the following order:

1) Chapter 1 comprises introduction of crypto currency and crypto currencies technology in the proposed work.
2) Chapter 2 explains the literature survey in the field of crypto currency mining farm for vehicles.
3) Chapter 3 explains about the project description and the methodology adopted in the noise free image restoration technique based on modified cuckoo search algorithm.
4) Chapter 4 deals with the performance of the projected noise free image restoration technique based on modified cuckoo search algorithm
5) Chapter 5 is conclusion and Future Scope of this research.

II. REVIEW OF LITERATURE

1) Title: The method for flexible management of block chain, based on crypto currencies markets and smart grids.
AUTHOR: Pierluigi Siano
YEAR : 2020
The growing trend in the use of block chain-based crypto currencies in modern communities provides several advantages, but also imposes several challenges to energy markets and power systems, in general. This paper aims at providing recommendations for efficient use of digital crypto currencies in today's and future smart power systems, in order to face the challenging aspects of this new technology. In this paper, existing issues and challenges of smart grids in the presence of block chain-based crypto currencies are presented and some innovative approaches for efficient integration and management of block chain-based crypto currencies in smart grids are proposed. Also some recommendations are given for improving the smart grids performance in the presence of digital crypto currencies and some future research directions are highlighted.

2) Title: Multistep assessment for crypto miners.
AUTHOR: Manic
YEAR : 2020
This paper proposes Manic (Multi-step Assessment for Crypto-miners), a system to detect Crypto Jacking websites. It uses regular expressions that are compiled in accordance with the API structure of different miner families. This allows the detection of crypto-mining scripts and the extraction of parameters that could be used to detect suspicious behaviour associated with Crypto Jacking. When Manic was used to analyse the Alexa top 1m websites, it detected 887 malicious URLs containing miners from 11 different families and demonstrated favourable results when compared to related Crypto Jacking research. We demonstrate that Manic can be used to provide insights into this new threat, to identify new potential features of interest and to establish a ground-truth dataset, assisting future research.

3) Title: A trust in block chain crypto currency ecosystem.
AUTHOR: Muhammad Habib Ur Rehman
YEAR: 2019
The recent growth in block chain-based crypto currency ecosystem has been attracting researchers, developers, investors, regulators, and speculators to develop new economic and business models for trade, investment, and taxation. Currently, the crypto currency ecosystem is immature with multifaceted trust issues at all levels from technology providers to users and governments. In this article, we present a detailed analysis of trust issues in the crypto currency ecosystem, including a detailed taxonomic discussion of the key trust aspects including price manipulation, price volatility, insider trading, parallel economy, shadow economy, reputation systems, transparency, centrality, token economy, governance, regulations, design, usability, privacy, and security. We also present a comparative analysis of the top 10 crypto currencies that are holding about 85% of the total market capital. Finally, we present a detailed summary of the key trust issues and their potential immediate, short-term, and long-term solutions. This article reveals that significant effort is required to develop a fully trustworthy crypto currency ecosystem.

4) Title: A Machine Learning methodology for Android malware detection and recognition, including crypto mining applications using the block chain.
AUTHOR: Cristiana Istrate
YEAR: 2019
The design is based on a hierarchical classification method, with several decision stages. A combination of functional and statistical features is proposed to be applied for data classification in order to provide a high-performance malware recognition process. The specific contribution of this design methodology is the hierarchical classifier with detection and discrimination stages, respectively. Further works should be done for various features sets in order to achieve an optimized and high-accuracy modeling process supporting an innovative Machine Learning-based solution for Android malware detection. Sun et al. utilized the Deep CNN-LSTM method to predict the soybean yield estimation. The Yield prediction was an immense consequence for yield mapping, harvest management, crop insurance, crop market planning, and remote sensing. The developed CNN-LSTM approach improved its practicability and feasibility in order to forecast the Particulate Matter (PM2.5) concentration was also verified in the model. The DNN structure was developed that integrated LSTM and CNN based on the historical data such as cumulated wind speed, duration of rain, and concentration of PM 2.5

The latest research in this area recommended that CNN could explore more spatial features and LSTM can reveal phonological features, which together play a significant role in crop yield prediction. However, the method employed histogram-based tensor alteration fused different remote sensing data which combined multisource data with a various resolution for feature extraction remained challenging.

5) Title: A secured crypto currency scheme based on post quantum block chain.
AUTHOR: Ying Sun
YEAR: 2018
Nowadays, block chain has become one of the most cutting-edge technologies, which has been widely concerned and researched. However, the quantum computing attack seriously threatens the security of block chain, and related research is still less. Targeting at this issue, in this paper, we present the definition of post-quantum block chain (PQB) and propose a secure crypto currency scheme based on PQB, which can resist quantum computing attacks. First, we propose a signature scheme based on lattice problem. We use lattice basis delegation algorithm to generate secret keys with selecting a random value, and sign message by preimage sampling algorithm. In addition, we design the first-signature and last-signature in our scheme, which are defined as double-signature. It is used to reduce the correlation between the message and the signature. Second, by combining the proposed signature scheme with block chain, we construct the PQB and propose this crypto currency scheme. Its security can be reduced to the lattice short integer solution (SIS) problem. At last, through our analysis, the proposed crypto currency scheme is able to resist the quantum computing attack and its signature satisfies correctness and one-more unforgeability under the lattice SIS assumption. Furthermore, compared with previous signature schemes, the sizes of signature and secret keys are relatively shorter than that of others, which can decrease the computational complexity. These make our crypto currency scheme more secure and efficient.

6) Title: Block chain standards for compliance and trust
AUTHOR: Anjum, Ashiq, Manu Sporny, and Alan Sill
YEAR: 2017
Methods for Flexible Management of Crypto currencies-based Crypto currencies in Electricity Markets and Smart Grids This paper aims at providing recommendations for efficient use of digital crypto currencies in today's and future smart power systems, in order to face the challenging aspects of this new technology. In this paper, existing issues and challenges of smart grids in the presence of crypto currencies-based crypto currencies are presented and some innovative approaches for efficient integration and management of crypto currencies-based crypto currencies in smart grids.

7) Title: Hardware Performance Counters for the Masses.
AUTHOR: Erven Rohou
YEAR: 2011
The paper proposes a Machine Learning methodology for Android malware detection and recognition, including crypto-mining applications using the crypto currencies. Method that classify based on the hierarchical classification, with several decision stages. A combination of functional and statistical features is proposed to be applied for data classification in order to provide a high-performance malware recognition process.

III. PROPOSED SYSTEM

A. Existing System

The automatic toll e-ticketing system is the approach used for the vehicle when it reaches the toll plaza, this is detected by using Infrared Proximity Sensor. In Existing System used CISC Mechanism method. Could not Store IOT webpage Manually they have to pay money for Toll e collection.

B. Proposed System

In this proposed system hereafter, all the next generation vehicles should come up with a new technology called Crypto Currency Mining Farm (CCMF) which will do Standalone Mining in the vehicle end and earn Crypto Currencies, This Crypto Currencies will be used for meeting all types of expenses for the Vehicle, it means Vehicle will earn Crypto Currencies and spend for all the listed expenses without disturbing the Vehicle owner.

The proposed concept contains two modules 1. CCMF in the vehicle 2. toll collection, CCMF is a device can be installed by any low voltage. Which will convert electrical energy to digital money. Tensilica's 32bit processer is used in crypto currency mining farm. Crypto currency mining farm will connect with internet, inside the vehicle and access the crypto currencies and will start the mining process and will earn the Crypto Currency and moves the Crypto Currency to the Digital Wallets. Figure 3.2 shows electric tollgate collection .This will be used for all expenses on the later stage and a Wi-Fi module is attached for the internet. Wi-Fi module with 2 relay is provided in the ETC side for toll gate access and EV charging. Once pay mode switch is pressed automatically the amount from the digital wallet from vehicle will transferred to the ETC as toll fee and something will be detected from our digital wallet. The same process will be followed for all the expenses like Charging and parking.

Globally Transportation charge is getting to an extreme high due to the demand of non-renewable resources like Petrol & Diesel, Electronic Toll Collection and Vehicle Parking Expenses all leads to make the travelling cost unaffordable. The automobile industry proposes new ideas like Electric Vehicle which will replace the usage of existing high-cost non-renewable resources like Petrol & Diesel, in the same way Automobile Industry proposes a new idea to reduce the Expenses of Electronic Toll Collection Charges, Vehicle Parking Expenses, and expenses like Electric Vehicle Charging Station Bills.

Crypto currency mining is the process that crypto currency use to generate a new coins. By mining we can earn crypto currency. And we can receive a crypto currency as a reward for completing blocks of verified transactions , which r add to crypto currencies. Block chain, as an immutable distributed ledger, is the underlying technology behind crypto currencies. The core elements of block chain include complex cryptographic functions for security and immutability, linear and nonlinear data structures to store, manage, and process crypto currency transactions. While crypto currencies helps to store correct data that is unaltered and permanent. Figure 3.1 describes the crypto currency mining farm kit.

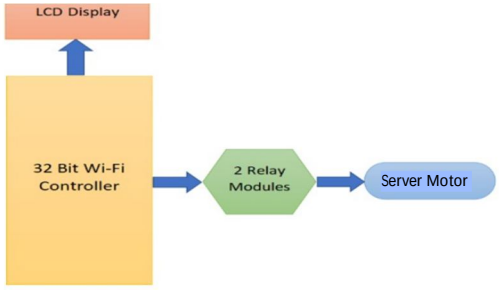


Figure 3.1 Crypto currency mining farm kit

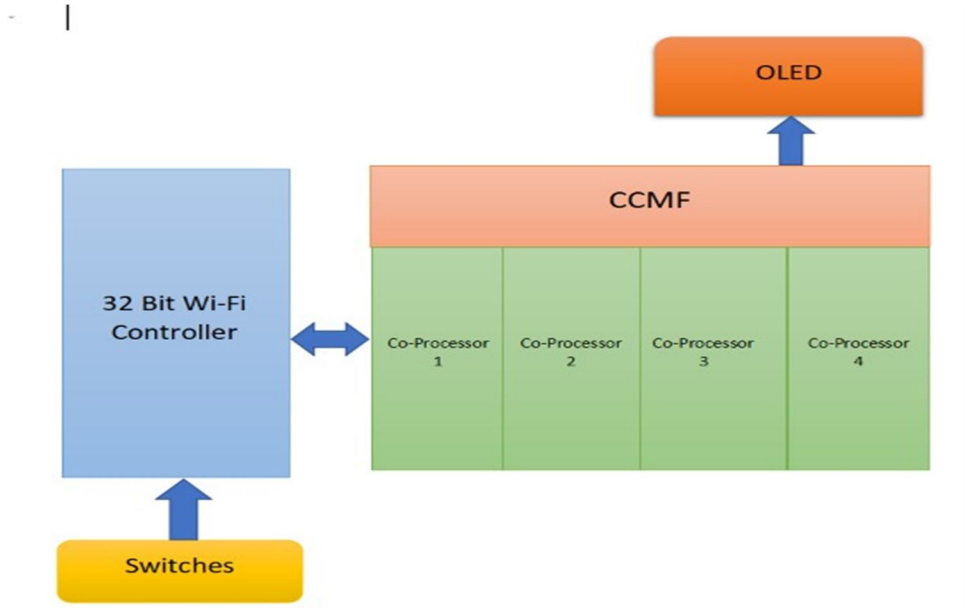


Figure 3.2 Electric Tollgate Collection

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

TABLE NO 3.3 TECHNICAL CONTRIBUTION OF INDIVIDUALS IN THE PROJECT

The three stages in the proposed work has been identified and contributed by the Individuals in the batch as follows:

Sl. No.	Module Name	Contributor Name	Description
1	CCMF, OLED and Coprocessor	Rohith Reddy V (0018121115)	a. Soldering the wifi Controller, Coprocessor and OLED components with the required wires to form the crypto currency mining farm kit. b. Arrangement of the components in quite efficient manner to provide power supply and to get connect internet to the wifi module to show the status like IP address in the OLED. c. Debugging the errors from the programming which was embedded into the wifi controller to verify the functionality.
2	32bit Wi-Fi Controller, Relay Module, DC Motor ,Payment Control Switches.	Revanth Krishna U (0018121122)	a. Simulation of the proposed work is done on the software and verifying its functionality with the help of hardware demo. b. Creating the webpage towards the ETC side in knowing the amount transaction within date and time of the particular event and to know the wallet balance and balance statistics after the transaction of the amount from the wallet. c. Embedded the code into the wifi controller and designing the 2 Relay modules as one for operating the DC Motor and another for charging purpose and then finally checking the status of the DC Motor to operate when the gate open status is displayed at LCD.
3	Simulation (Software equipment) and LCD display	Mohan Reddy K (0018121123)	a. Arduino programming is done in the ardinodroid software and then simulating the proposed work in the proteus software. b. Debugging the errors of the Arduino programming to run and compile successfully and finding a path of programming to use that in simulation part of proteus software. c. Connecting the LCD display to the wifi controller in order to display the status of charging ON & OFF and Gate open & Gate close with the help of payment control switch.

As a final process, everyone was involved in integrating all the module codes and final simulation result was obtained which illustrates the proposed crypto currency mining farm for vehicles has given accurate application of real time scenario. On successful connection and arrangement of all the components helps in producing the good experimental results and better performance of web page regarding the duino coins.

The work carried out by the individuals in the batch are explained in the following sections.

C. 32 BIT wifi controller

32-In the computer world, 32-bit and 64-bit refer to the type of central processing unit, operating system, driver, software program, etc. From entry-level to high-performance options, our 32-bit MCUs have the features and flexibility to help you create advanced solutions for the latest applications. It is a low-power system. From entry-level to high-performance options, our 32-bit MCUs have the features and flexibility to help you create advanced solutions for the latest applications. Use the links below to find the product family that matches your design requirements.

The name '32-bit microcontroller' implies that the microcontroller is capable of handling arithmetic operation for a 32-bit value. Compared to an 8-bit microcontroller, the 32-bit microcontroller takes fewer instruction cycles to execute a function due to its wider data bus. 32-bit is a type of CPU architecture that is capable of transferring 32 bits of data per clock cycle. In more technical terms, this means processors can work with 32-bit binary numbers (decimal number up to 4,294,967,295). Anything larger and the computer would need to break the data into smaller pieces.

Features of 32-bit WIFI Controller

1) *Wi-Fi Module – ESP-12E module similar to ESP-12 module but with 6 extra GPIOs.*
2) *USB – micro-USB port for power, programming and debugging*
3) *Headers – 2x 2.54mm 15-pin header with access to GPIOs, SPI, UART, ADC, and power pins Misc – Reset and Flash buttons*
4) *Power – 5V via micro-USB port*
5) *Dimensions* – 49 x 24.5 x 13mm

D. Crypto Currency Mining Farm (CCMF)

The brand name Tensilica is a combination of the word Tensile, meaning capable of being extended, and the word Silica from silicon, the element of which integrated circuits are primarily made.Figure 3.4 shows the crypto currency mining farm kit. It is highly used in crypto hash function for the crypto currencies. FToday's smart connected world with pervasive intelligence at edge nodes for smart sensory computing is driving the requirements for higher bandwidths and increased compute complexity and throughput. Designers using traditional approaches like general-purpose CPUs and DSPs, FPGAs, and dedicated fixed RTL are experiencing several roadblocks such as lower performance and data throughput due to the use of bus interfaces, high power consumption, and lack of programming flexibility for future-proofing, longer time to market, and so on. Cadence Tensilica processor technology offers to overcome these roadblocks and bring innovation to the forefront.

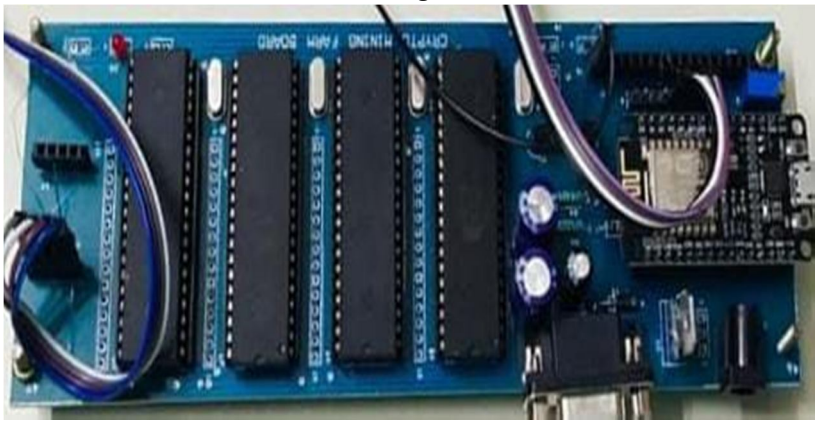


Figure 3.4 Crypto currency Mining Farm Kit

IV. RESULT AND DISCUSSIONS

This section presents the results of the proposed method of crypto currency mining farm for vehicle.

A. Experimental Setup

The following figure is the experimental setup of the proposed work in which the crypto currency mining farm kit can be prepared by integrating the wifi module, coprocessors and OLED and the power supply is given to the kit from the external source separately payment control switches are designed in the board to operate along with CCMF kit as shown in the figure 4.1.

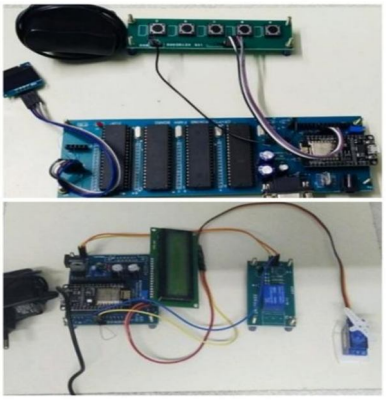


Figure 4.1 Experimental Setup

B. Experimental Results

After setup the experiment, power supply is given to the 2 boards to get the experimental results. Figure 4.2,Figure 4.3,Figure 4.4,Figure 4.5 shows the experimental results.

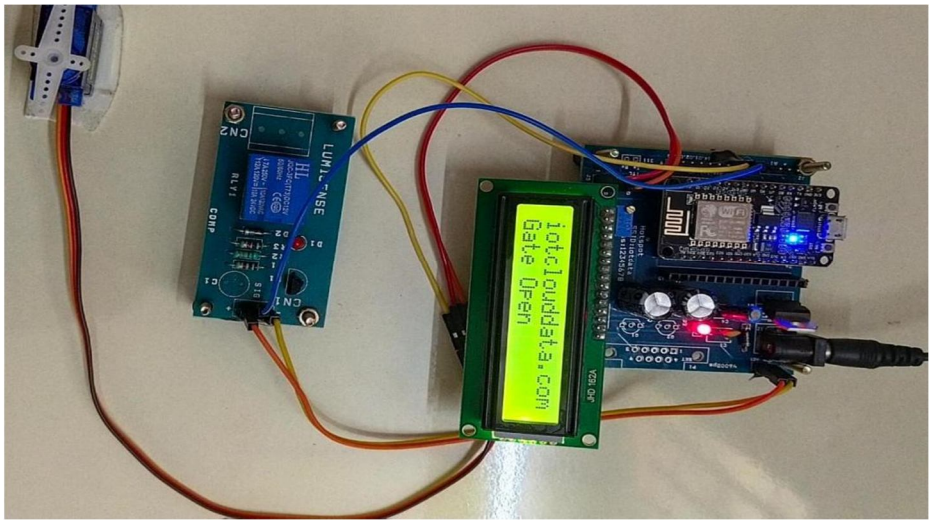


Figure 4.2 Gate open

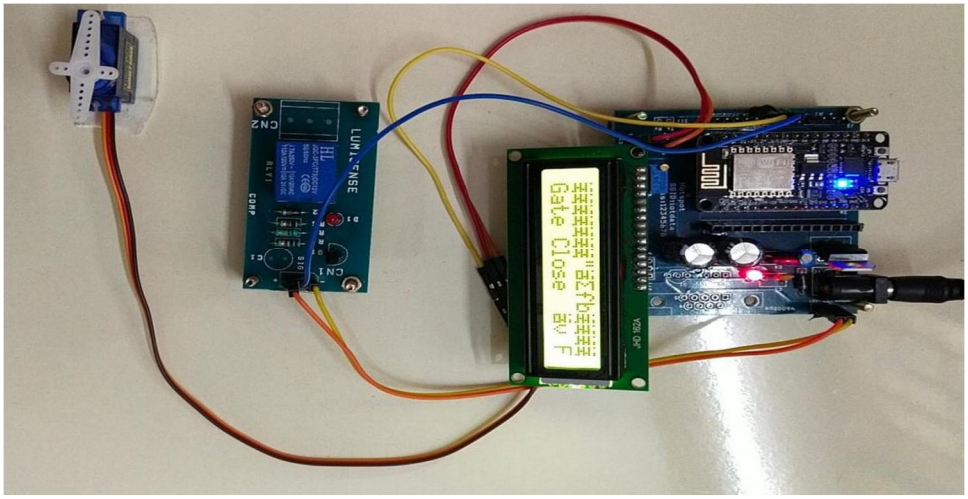


Figure 4.3 Gate close

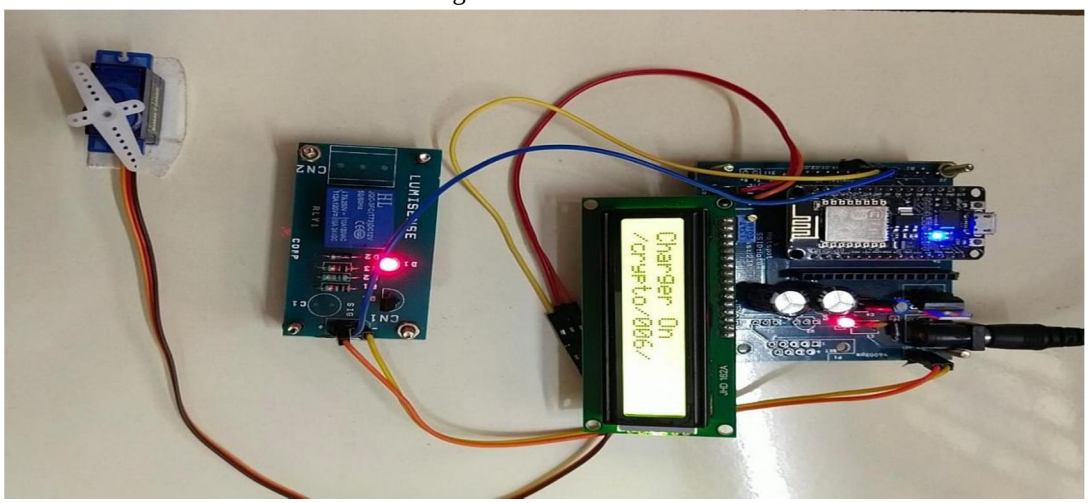


Figure 4.4 Charging on

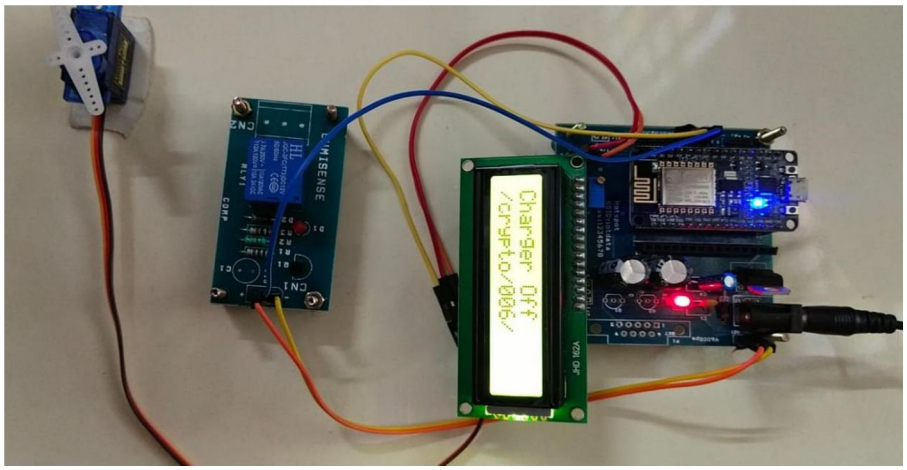


Figure 4.5 Charging off

C. Performance Analysis

Performance analysis is shown from the webpage creation of the proposed work. In our work duino coin –web wallet is used for crypto currency mining farm. Figure 4.6, Figure 4.7, Figure 4.8 shows performance analysis.

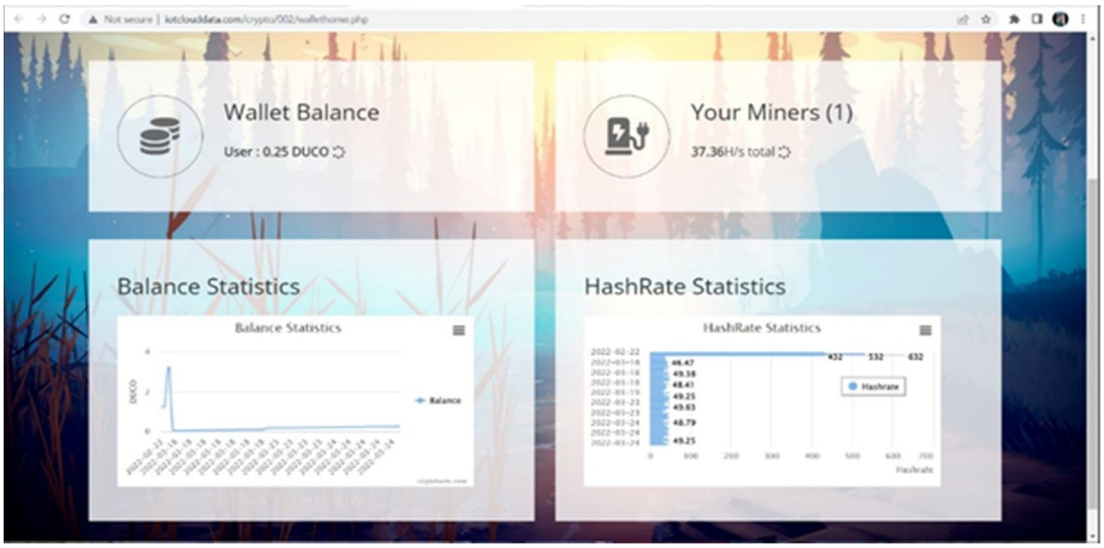


Figure 4.6 Digital wallet

As a part however the real life application is happening that a toll gate is opened, once the amount is payed or else once the amount is debited from our wallets. In such a manner, In our proposed work a prototype is created to work on the same principle.

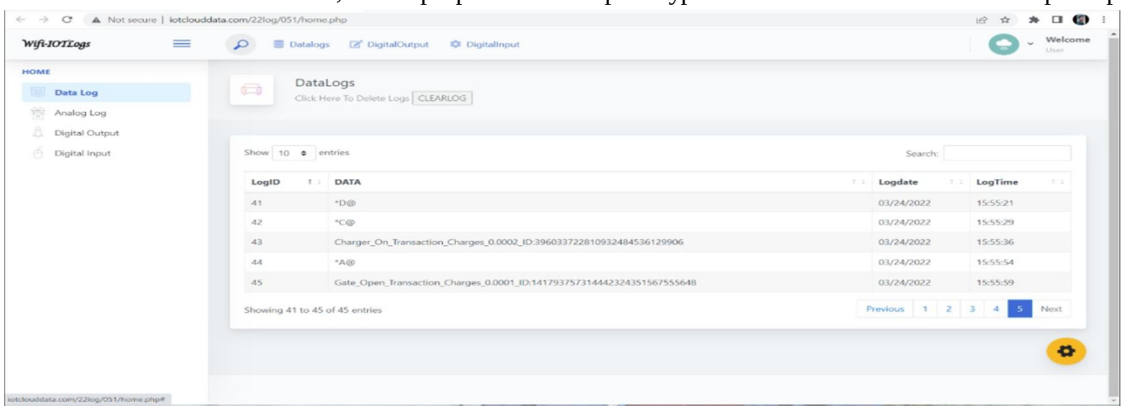


Figure 4.7 Transaction Charges

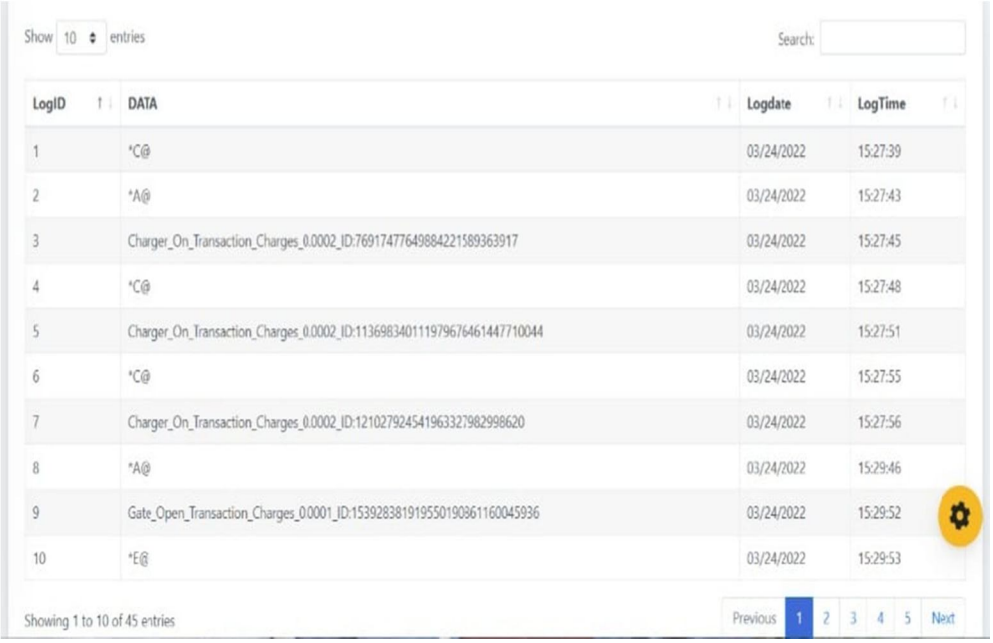


Figure 4.8 Transaction Charges with log time and date

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Nowadays, block chain has become one of the most cutting-edge technologies, which has been widely concerned and researched. Targeting at this issue, in this paper, we present the definition of post-quantum block chain (PQB) and propose a secure crypto currency scheme based on PQB, which can resist quantum computing attacks. We use lattice basis delegation algorithm to generate secret keys with selecting a random value, and sign message by preimage sampling algorithm. It is used to reduce the correlation between the message and the signature. Second, by combining the proposed signature scheme with block chain, we construct the PQB and propose this crypto currency scheme. Its security can be reduced to the lattice short integer solution (SIS) problem. At last, through our analysis, the proposed crypto currency scheme is able to resist the quantum computing attack and its signature satisfies correctness and one-more unforgeability under the lattice SIS assumption. Furthermore, compared with previous signature schemes, the sizes of signature and secret keys are relatively shorter than that of others, which can decrease the computational complexity. These make our crypto currency scheme more secure and efficient.

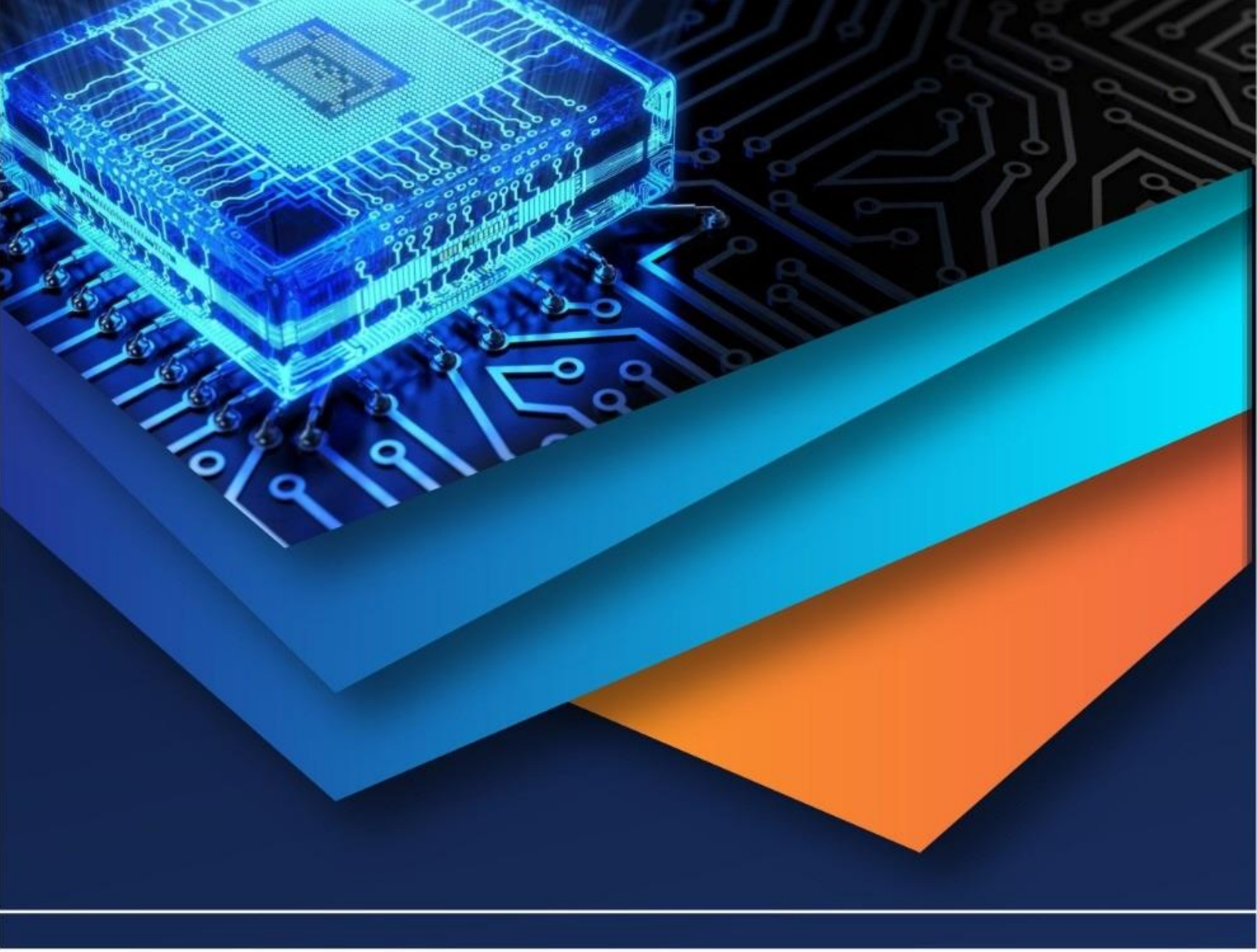
B. Future Scope

In this system hereafter all the next generation vehicles should come up with a new technology called Crypto Currency Mining Farm (CCMF) which will do Standalone Mining in the vehicle end and earn Crypto Currencies, This Crypto Currencies will be used for meeting all types of expenses for the Vehicle, it means Vehicle will earn Crypto Currencies and spend for all the listed expenses without disturbing the Vehicle owner.

REFERENCES

[1] S. Arshad, A. Khan, M. A. Shah and M. Ahmed. 2016. Android Malware Detection & Protection: A Survey, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2.
[2] R. Raveendranath, R. Venkiteswaran and A. J. Babu. 2014. Android Malware Attacks and Countermeasures: Current and Future Directions
[3] Malwarebytes LABS: State of Malware Report 2017 https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf
[4] R. Sato, D. Chiba, and S. Goto. 2013. Detecting Android Malware by Analyzing Manifest Files, Proceedings of the Asia-Pacific Advanced Network 2013, pp. 23–31,
[5] C.-Y. Huang, Y.-T. Tsai, and C.-H. Hsu. 2013. Performance Evaluation on Permission-based Detection for Android Malware, Adv. Intell. Syst. Appl. - Vol. 2, vol. 21, pp. 111–120,
[6] N. V. Duc, P. T. Giang and P. M. Vi. 2015. PERMISSION ANALYSIS FOR ANDROID MALWARE DETECTION, The Proceedings of the 7th VAST - AIST Workshop "Research Collaboration: Review and perspective".
[7] A. Skovoroda and D. Gamayunov. 2015. Securing mobile devices: malware mitigation methods, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 2.

[8] O. Yeshvekar, S. Zende, D. Walvekar, N. Wabale, A. Korde, M. Saravanapriya, N. S. Patil. 2015 . A Survey of Evaluation Techniques for Android Anti-Malware using Transformation Attacks, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 11,
[9] V. Rastogi, Y. Chen and X. Jiang. 2014. Catch Me if You Can: Evaluating Android Anti-malware against Transformation Attacks, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,
[10] L. Weichselbaum, M. Neugschwandtner, M. Lindorfer, Y. Fratantonio, V. Veeny and C. Platzer. 2014. ANDRUBIS: Android Malware Under the Magnifying Glass, TECHNICAL REPORT TRISECLAB-0414-001,
[11] C. Jarabek, D. Barrera and J. Aycock. 2012. ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware, ACSAC '12 Dec. 3- 7, Orlando, Florida USA
[12] S. Alam, R. Riley, I. Sogukpinar and N. Carkaci. 2016. DroidClone: Detecting Android Malware Variants by Exposing Code Clones
[13] R. Andriatsimandetra and V. V. Triem Tong. Nov 2015, Detection and Identication of Android Malware Based on Information Flow Monitoring, The 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015), New York, United States
[14] S. Hou, Y. Ye, Y. Song and M. Abdulhayoglu. 2017. HinDroid: An Intelligent Android Malware Detection System Based on Structured Heterogeneous Information Network, Proceedings of KDD'17, August 13-17, Halifax, NS, Canada
[15] G. Kapse and A. Gupta. 2015. Detection of Malware on Android based on Application Features, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4), 3561- 3564
[16] M. Leeds, M. Keffeler and T. Atkison. 2017. Examining Features for Android Malware Detection, Int'l Conf. Security and Management | SAM'17
[17] J. Sahs and L. Khan. 2012. A Machine Learning Approach to Android Malware Detection, 2012 European Intelligence and Security Informatics Conference
[18] B. Baskaran and A. Ralescu. 2016. A Study of Android Malware Detection Techniques and Machine Learning, MAICS 2016
[19] Y. Kim, K. J. Liszka and C. C. Chan. 2016. Using DroidDream Android Malware Behavior for Identification of Other Android Malware Families, Int'l Conf. Security and Management, SAM'16
[20] K. Alzaylaee, Y. Yerima and S. Sezer. 2017. EMULATOR vs REAL PHONE: Android Malware Detection Using Machine Learning, IWSPA 2017 Proceedings of the 3rd ACM International Workshop on Security and Privacy Analytics, co-located with CODASPY'17, pages 65-72, Scottsdale, Arizona, USA - March 24 – 24
[21] Pierluigi Siano(2020) proposed the method for flexible management of block chain, based on crypto currencies markets and smart grids.
[22] Manic (2020) proposed a multistep assessment for crypto miners. This paper proposes Manic (Multi-step Assessment for Crypto-miners), a system to detect Crypto Jacking websites.
[23] Muhammad Habib Ur Rehman(2019) proposed a trust in block chain crypto currency ecosystem.
[24] Cristiana Istrate(2019) proposed a Machine Learning methodology for Android malware detection and recognition, including crypto-mining applications using the block chain.
[25] Ying Sun (2018) proposed a secured crypto currency scheme based on post quantum block chain.
[26] Anjum, Ashiq, Manu Sporny, and Alan Sill (2017) Block chain standards for compliance and trust .
[27] Erven Rohou (2011) Tiptop: Hardware Performance Counters for the Masses. Android Malware Detection and Crypto-Mining Recognition Methodology with Machine Learning.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY