A project report on

Blockchain Based

Mobile Theft Detection and Event Monitoring

By

Sadam Hussain Ganie (23CSM2R20)

Under the supervision of

Dr. E Suresh Babu

Assistant professor

Department of Computer Science and Engineering

Academic year 2023-24

II semester

National Institute of Technology, Warangal

Table of contents

ABSTRACT…… 4
1. Introduction 4
2. Background and Related Work 5
3. Methodology 8
4. Results 12
5. Algorithms 20
6. Conclusion 21
7. References 21

List of Figures

Figure 1: High overview of blockchain. 9
Figure 2: Flowchart of the methodology. 11
Figure 3: Proposed system architecture. 12
Figure 4: Structure of device instance in smart contract. 12
Figure 5: Structure of user instance in smart contract. 13
Figure 6: Blockchain storage. 13
Figure 7: Blockchain transaction. 14
Figure 8: Mined block. 14
Figure 9: Index page. 15
Figure 10: User registration page. 15
Figure 11: Login page. 15
Figure 12: User dashboard. 16
Figure 13: Purchased device. 16
Figure 14: Unsold device. 17
Figure 15: Device registration. 17
Figure 16: Device listed on user dashboard. 18
Figure 17: Fetch location. 18
Figure 18: Device listing. 19
Figure 19: Lost devices. 19
Figure 20: Logout page. 19
Figure 21: Manufacturer's device registration algorithm. 20
Figure 22: Purchase a device algorithm. 20
Figure 23: Ownership transfer algorithm. 20
Figure 24: Reporting loss algorithm. 21

ABSTRACT

In today's digitally connected world, mobile devices have become indispensable tools for communication, work, and entertainment. However, the ubiquitous nature of these devices also exposes them to the risk of being lost or stolen, potentially leading to unauthorized access and misuse of personal information. To address this challenge, there is a pressing need for a robust system that can track lost or stolen devices and provide timely notifications to their rightful owners, including crucial information such as device location.

In response to this need, our project focuses on leveraging blockchain technology to develop a comprehensive mobile theft detection and event monitoring system. By registering all devices on a blockchain network, we establish a secure and transparent platform for managing device-related operations such as purchases, sales, and tracking lost or stolen devices. Blockchain's decentralized nature and consensus mechanism ensure the integrity and immutability of data, thereby enhancing the security and reliability of the system.

Through our work, we aim to create a flexible and innovative solution that surpasses traditional methods of mobile theft prevention. By harnessing the power of blockchain, our system offers a revolutionary approach to safeguarding mobile devices and ensuring the peace of mind of their users in an increasingly digital world.

1. Introduction

In this project, we thoroughly studied and implemented two modules:

Module 1: Alert Propagation in Blockchain Systems, and

Module 2: Theft Detection and Event Monitoring.

Mobile phones have become indispensable in today’s digital era, serving both personal and professional needs. However, the increase in dependency on mobile phones has led to an alarming rise in mobile thefts or losses, resulting in data loss and compromised user privacy. Research studies reveal that approximately 70 million smartphones are lost(or stolen) each year, with less than 7% of them being recovered [1]. Furthermore, company-issued phones are not immune to these breaches, with 4.3% of them being lost or stolen annually. Workplaces and conference environments are the primary locations for mobile thefts, with the number of incidents increasing by 39.2% between 2019 and 2021 [2]. Given this alarming situation, there is an urgent need for mobile theft prevention techniques that can safeguard user data and privacy. Blockchain technology holds great potential to address the mobile theft detection problem. With its decentralized and immutable nature, blockchain can help retrieve lost or stolen smartphones, or at the very least, prevent misuse by unauthorized parties.

Although blockchain technology has not been widely adopted nationally or internationally for mobile theft detection, many companies are exploring its use for mobile security and anti-theft solutions. Internationally, companies like Samsung and Huawei are conducting research on the use of blockchain technology for mobile security, with Samsung filing several patents for blockchain-based mobile security solutions [3, 4].

Mobile theft does not pose financial loss only but these incidents pose significant threats to personal privacy and security. Adversaries can exploit stolen devices to access sensitive data, including personal photos, messages, financial information, and login credentials. According to a Norton Symantec poll, 53 percent of people in India, 33 percent of consumers in Canada, and 36 percent of consumers in the United States had experienced cell phone loss or theft [14].

To address these challenges and protect users' sensitive data, it is crucial to implement effective security measures. In response, we propose a model that leverages blockchain-based technology to prevent data leakage in the event of a lost or stolen mobile device.Our proposed solution utilizes blockchain technology and smart contracts to securely store and manage sensitive data. By encrypting and decentralizing data storage, our model ensures that confidential information remains protected even if a device falls into unauthorized hands [15].

Through the implementation of this blockchain based approach, we aim to provide users with peace of mind knowing that their data is safeguarded against potential threats posed by mobile theft. By mitigating the risks associated with data leakage, our model contributes to enhancing overall mobile security and protecting users' privacy in an increasingly interconnected world [16].

Therefore, in this report, we present how blockchain technology can be utilized for anti-theft and mobile security purposes, leveraging its decentralized, secure, transparent, and trustworthy nature [5]. We will delve into how blockchain and smart contracts can securely store user data, authenticate users, and detect unauthorized individuals attempting to register stolen or lost phones.

2. Background and Related Work

Biometric-based solutions such as facial recognition and remote wiping systems can restrict strangers from gaining access to someone's smartphone. However, these measures do not fully prevent mobile theft. In their study [6], researchers have proposed an innovative anti-theft system based on walking style recognition. This system, named "Virtual Safe," alerts the device owner if it detects a different walking style from that of the owner. The software utilizes the phone's accelerometer to monitor movement and compares the current walking style to that of the owner, promptly notifying the owner if any discrepancies are detected. In their study [7], the authors proposed an anti-theft solution based on locking and unlocking the SIM card. Users have the option to lock the SIM card when the device is lost or stolen and set an unlocking code, which both locks

the SIM and the phone. When the device is turned on by someone else, it checks whether the SIM card is locked. If it is locked, the device prompts the user to enter the unlocking code. If the correct code is entered, the device starts up; otherwise, it remains inactive. In their study [8], the authors proposed a BIOS-based solution that can detect theft even if the device is turned off. This solution utilizes BIOS cells to store GPS information, ensuring that location data is retained even if the SIM card and battery are removed from the device. In their study [9], the authors proposed an anti-theft solution based on motion trajectory and user characteristics. By utilizing device sensors such as the accelerometer, gyroscope, and other sensors, data can be collected from the phone and combined with the habitual use patterns of the owner. This system can determine whether the phone is being carried by its actual owner and notify the owner accordingly. In their study [10], the authors proposed a mechanism involving the development of software that needs to be installed on a mobile phone. This software, when installed, captures photos whenever the SIM card is changed and sends the snapshots to an alternate number as MMS and to an email address. This approach aids in detecting thieves by providing visual evidence of unauthorized SIM card changes.

Blockchain is a distributed, append-only, peer-to-peer network that consists of a chain of blocks. Each block stores a set of transactions and is linked to the previous block. Once transactions are committed, they cannot be modified. Smart contracts, which are blockchain-based programs, execute when certain conditions are met and automate processes on the blockchain.

The HyperLedger Fabric platform is a blockchain framework that ensures all participating users are authenticated and offers versatility for a variety of industry use cases[11]. With advanced privacy controls, HyperLedger Fabric can enhance transparency and traceability of transactions within the network.

The use of Blockchain technology provides an efficient solution for preventing mobile theft and data loss [12]. This technology offers a decentralized and tamper-proof method to track stolen devices and prevent their resale. Blockchain, being decentralized, stores accurate information across nodes, making data tampering nearly impossible [13]. For our project, we will utilize a private blockchain connecting mobile manufacturing companies and their nodes.

Furthermore, smart contracts will ensure robust and automated processes, minimizing human errors. Blockchain technology facilitates cross-border cases more effectively than current solutions. Current solutions, such as those mentioned in [10], have serious privacy concerns that blockchain technology can address. Reducing mobile thefts through blockchain technology will lead to cost reductions and positive economic impacts.

The Mobile Theft Identification project aims to create a robust system for detecting and identifying stolen mobile devices while closely monitoring related events. This project seamlessly integrates IoT modules into mobile phones, allowing for the collection of critical data such as device location, status, and user activities. The foundation of secure device identity management relies on the Hyperledger Fabric blockchain platform, ensuring the utmost level of data security and integrity. In case of theft or suspicious

activities, the system promptly responds by triggering real-time alerts and maintaining continuous surveillance of device related events. These alerts are instantly communicated to authorized personnel, facilitating the tracking and potential recovery of stolen devices. The Mobile Theft Identification project seeks to significantly enhance mobile device security, increase the likelihood of recovering stolen devices, and offer real time event monitoring capabilities. Here, I am going to discuss the functionality of our project, which serves as the backbone in detecting and preventing mobile theft while ensuring the security of sensitive data stored on mobile devices.

Alert Triggering: The system is designed to promptly respond to theft incidents or any suspicious activities related to mobile devices. When a theft is reported or detected, the module triggers real-time alerts to notify relevant parties.

Continuous Monitoring: The module maintains constant surveillance of events related to mobile devices, including device location, & login attempts.

Real-time Notifications: Authorized personnel receive real-time notifications about events of interest. This ensures that any unusual or potentially security threatening actions are promptly addressed.

This proactive approach enhances security, increases the chances of device recovery, and provides valuable insights into device usage and potential. Following are the details of some tools and technologies that are utilized to complete this project.

2.1 Truffle

Truffle is a development framework for Ethereum that provides developers with a suite of tools for building, testing, and deploying smart contracts. It simplifies the process of smart contract development by offering features such as automated contract compilation, testing, and deployment scripts. Truffle also includes a built-in development environment and a configurable build pipeline to streamline the development workflow.

2.2 Ganache

Ganache is a personal blockchain emulator developed by Truffle. It allows developers to create a local Ethereum blockchain environment for testing and development purposes. Ganache provides a user-friendly interface for managing accounts, deploying contracts, and inspecting blockchain state. It offers features like instant mining, gas price control, and customizable blockchain configurations to simulate real-world blockchain scenarios without the need for a live network.

2.3 Node.js

Node.js is a runtime environment that allows developers to run JavaScript code outside of a web browser. It uses the V8 JavaScript engine to execute code server-side, enabling the development of scalable and high-performance applications. Node.js is commonly used for building backend APIs, web servers, and command-line tools. It offers a vast ecosystem of libraries and frameworks, making it a popular choice for building server-side applications.

2.4 Solidity

Solidity is a high-level programming language specifically designed for writing smart contracts on the Ethereum blockchain. It is statically typed and supports inheritance, libraries, and complex user-defined types. Solidity code is compiled into bytecode that can be executed on the Ethereum Virtual Machine (EVM). It provides features such as modifiers, events, and error handling to facilitate the development of secure and efficient smart contracts.

2.5 Metamask

Metamask is a browser extension that serves as a cryptocurrency wallet and Ethereum gateway. It allows users to interact with Ethereum-based decentralized applications (DApps) directly from their web browsers. Metamask provides a secure and convenient way to manage Ethereum accounts, sign transactions, and access blockchain-based services. It also offers features like token management, decentralized identity, and integration with external wallets and hardware devices.

3. Methodology

Each mobile phone can be registered by the manufacturing company with a unique identifier, such as the International Mobile Equipment Identity (IMEI) number. When a device is purchased by a user, the company inserts a transaction into the blockchain indicating the purchase and updating the owner of the device. Other parameters, such as the “status of the device”, are also updated, with possible values including “Sold”, “lost/theft”, “Not sold”. Initially, when a device is manufactured, its status is set to “Not sold”. When a legitimate user purchases the device, the status is updated to “Sold”, and if the device is lost or stolen, the legitimate owner can update the status to “Lost/theft”. The immutable property of the blockchain ensures that unauthorized users cannot claim ownership of a stolen device, as tampering with the entire blockchain is nearly impossible. Additionally, the blockchain can track other information, such as the location of devices using GPS trackers. This location data can aid in detecting the thief. Smart contracts automate operations such as “sell”, “purchase”, and “report theft”. If a device is purchased by a user from a previous owner, the history of owners is maintained in the blockchain. This ensures that only legitimate devices are available in the market, and illegal devices cannot be sold or purchased. Location-based tracking can send signals to the owner who reported the device as lost, enabling them to track the device’s location.

Figure 1 represents the high level overview of how the proposed system works. The manufacturers, & end users request a transaction which is broadcasted to peer-to-peer network where the transaction is validated by the network of nodes using a validation engine. The verified transaction is combined with other transactions to create a block, which is later added to the blockchain. This is stored in a storage engine as shown in the figure below.

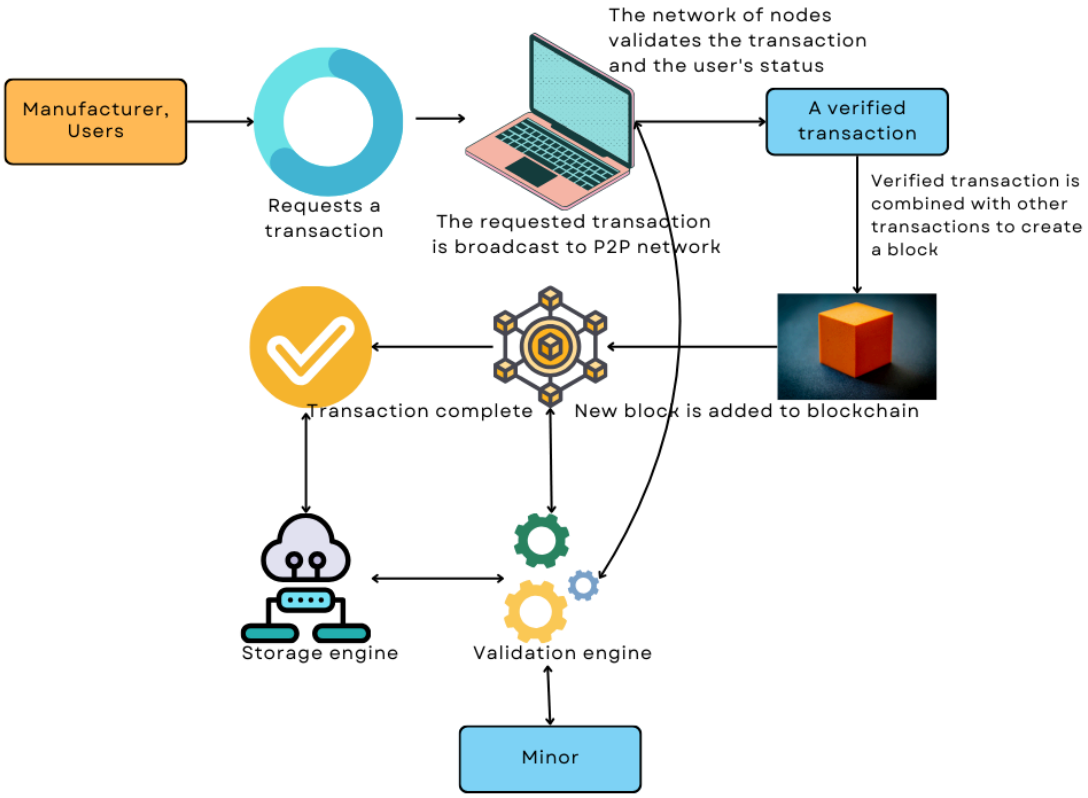

Figure 1: High overview of blockchain.

Initially, users are required to register on the system by providing essential information such as their name, email address, etc. Once successfully registered within the blockchain network, users gain access to login functionalities. Manufacturers can subsequently register mobile devices within the blockchain system by inputting details like the device's IMEI number, name, model, location, and image. These registered devices are then publicly displayed on the website, allowing users to browse and potentially purchase them. At the outset, these devices are listed as "Not sold".

Users logged into the system can view the available devices for sale and make purchases accordingly. Only devices in the "Not sold" and "Not lost" states are eligible for purchase. Following a successful transaction, purchased devices are displayed on the user's dashboard with their respective statuses. Users have the flexibility to buy multiple devices and can also mark devices as lost or stolen. However, only the owners of devices, with a status of "sold", can initiate the process of marking a device as stolen. Once marked as stolen, further actions on the device are restricted, and its location is continuously monitored and relayed to the owner. Lost devices are separately displayed on a dedicated "lost devices" dashboard.

Owners are provided with the option to transfer device ownership to another authenticated user, akin to selling the device. Additionally, the system incorporates robust security measures, including secure login and logout functionalities, to safeguard user data and transactions.

Following are the different operations allowed in the network:

3.1 Registration

Users begin by registering on the system by providing necessary details such as name, email address, etc. This information is securely stored within the blockchain network.

3.2 Login

Once registered, users can log in to the system using their credentials, gaining access to various functionalities.

3.3 Device Registration

Manufacturers can register mobile devices within the blockchain system by inputting essential details such as IMEI number, device name, model, location, and image. These registered devices are publicly displayed on the website for potential buyers.

3.4 Device Purchase

Logged-in users can browse the available devices for sale and make purchases as desired. Devices listed as "Not sold" are eligible for purchase. Upon successful transactions, purchased devices are added to the user's dashboard, displaying their respective statuses.

3.5 Mark as Lost/Stolen

Users have the option to mark devices as lost or stolen. However, only owners of devices with a "sold" status can initiate this process. Once marked, the device's status is updated accordingly, and further actions on the device are restricted. The system continuously monitors and relays the device's location to the owner.

3.6 Transfer Ownership

Device owners can transfer ownership to another authenticated user, similar to selling the device. This operation involves updating ownership details in the blockchain, ensuring a secure transfer process.

3.7 User Dashboard

The user dashboard provides a personalized view of the user's activities and device inventory. It displays purchased devices, their statuses, and any relevant information.

3.8 Login/Logout

Robust security measures are incorporated into the system, including secure login and logout functionalities. Users are required to authenticate themselves before accessing the system, and proper logout procedures ensure the security of user accounts and data.

3.9 Lost Device Dashboard

A dedicated dashboard is designed to display lost or stolen devices separately. This allows users to identify and avoid purchasing devices with compromised statuses,

enhancing security and transparency within the system.

3.10 Location Monitoring

Location of lost devices is monitored and reported to its owner. Users can login and view the location information of lost devices on the dashboard.

Overall, these operations collectively contribute to the functionality and security of the mobile theft detection and event monitoring system, providing users with a seamless and reliable experience.

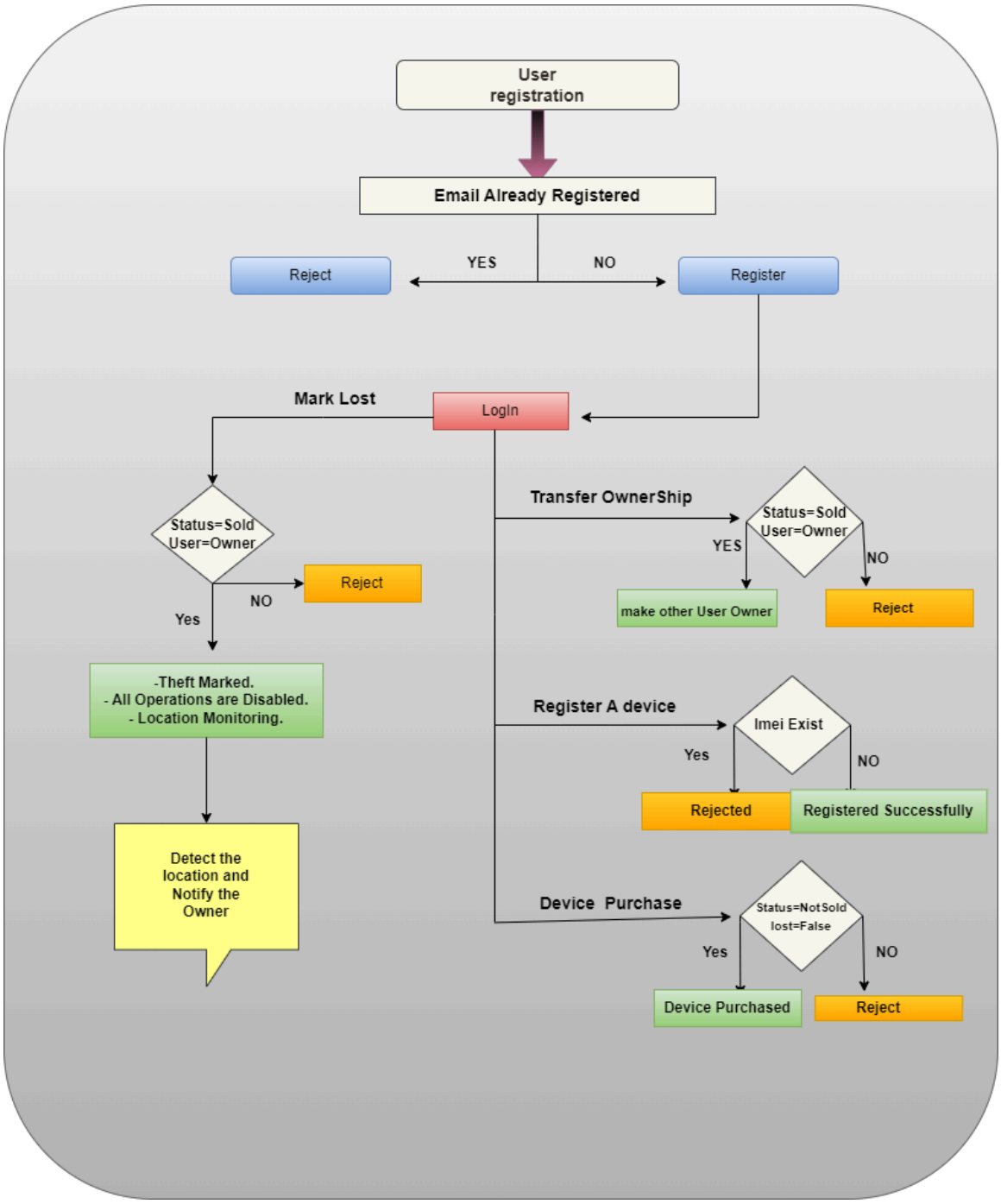

Figure 2: Flowchart of the methodology.

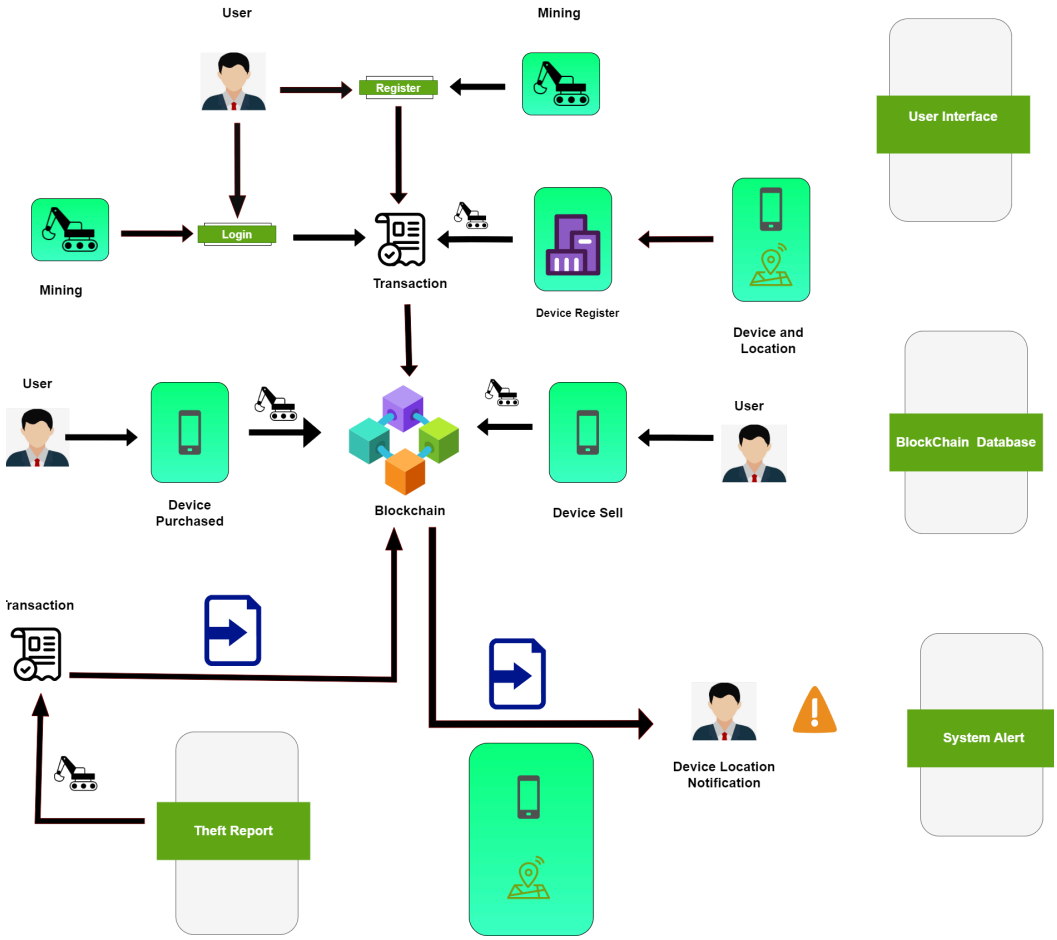

Figure 3: Proposed system architecture.

Figure 2 shows the flowchart of the proposed system where different operations are explained. Figure 3 represents the architecture of the proposed system which illustrates how users interact with the blockchain system, perform device transactions, and contribute to mining while ensuring security and transparency through blockchain technology.

4. Results

Figure 4 shows the structure of mobile devices in the blockchain. Details like device name, device IMEI, location, image, sold flag, lost flag, owner hash address, device identifier, email address of device owner.

```
struct device {
    string name;
    string imei;
    string location;
    string imageUrl;
    bool sold;
    bool lost;
    address owner;
    uint deviceId;
    string email;
}
device[] public devices;
```

Figure 4: Structure of device instance in smart contract.

Figure 5 shows the structure of users in the smart contract. It shows how the user details are stored in the blockchain network. Details like user email, password, address, country, zip code, name, location - latitude and longitude are stored in the blockchain storage to keep track of authentic users. The email address is unique and the duplicated entries are not allowed by the network. Location represents the location of the lost device associated with the user. When a user wants to fetch the location of any device, the same is shown on frontend and stored in blockchain as well.

```
struct user {
    //email, password, address, country, zip, name;
    string email;
    string password;
    string address_;
    string country;
    string zip;
    string name;
    string lat;
    string lon;
}
```

Figure 5: Structure of user instance in smart contract.

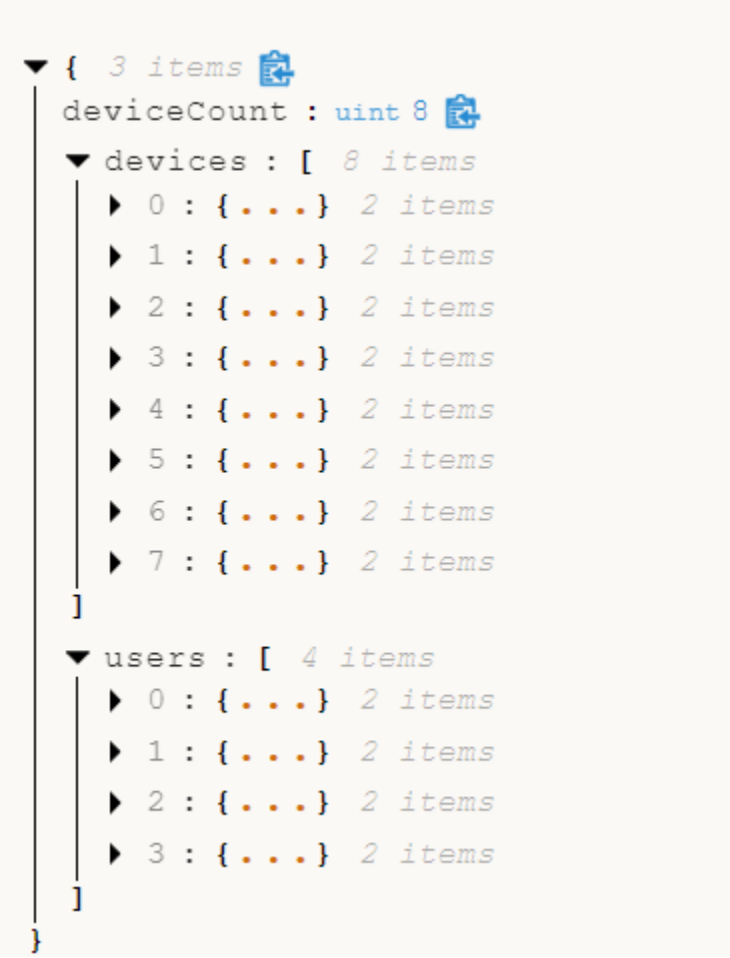

Figure 6: Blockchain storage

Figure 6 shows the storage of the blockchain in Ganache. The devices, users, and device count is stored.

Figure 7: Blockchain transaction.

Figure 7 shows a detailed view of one of the transactions associated with “mark lost” operation. Device with deviceId 1 is marked lost by its owner sh23csm2r20@student.nitw.ac.in as shown in the figure.

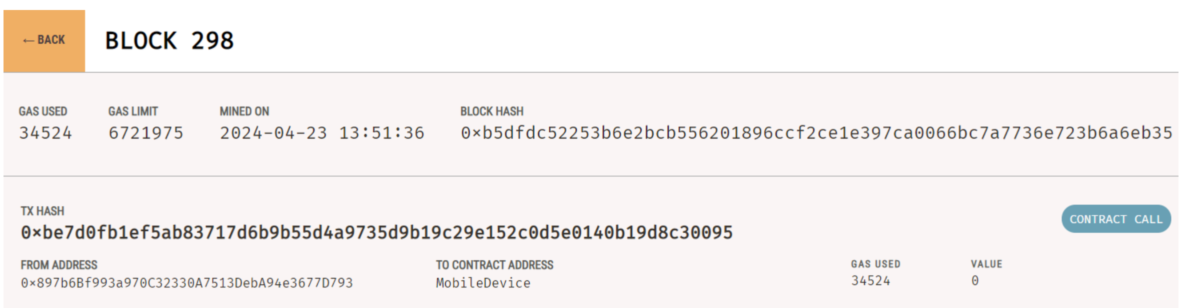

Figure 8: Mined block. This figure shows the details of block number 298 mined in the blockchain.

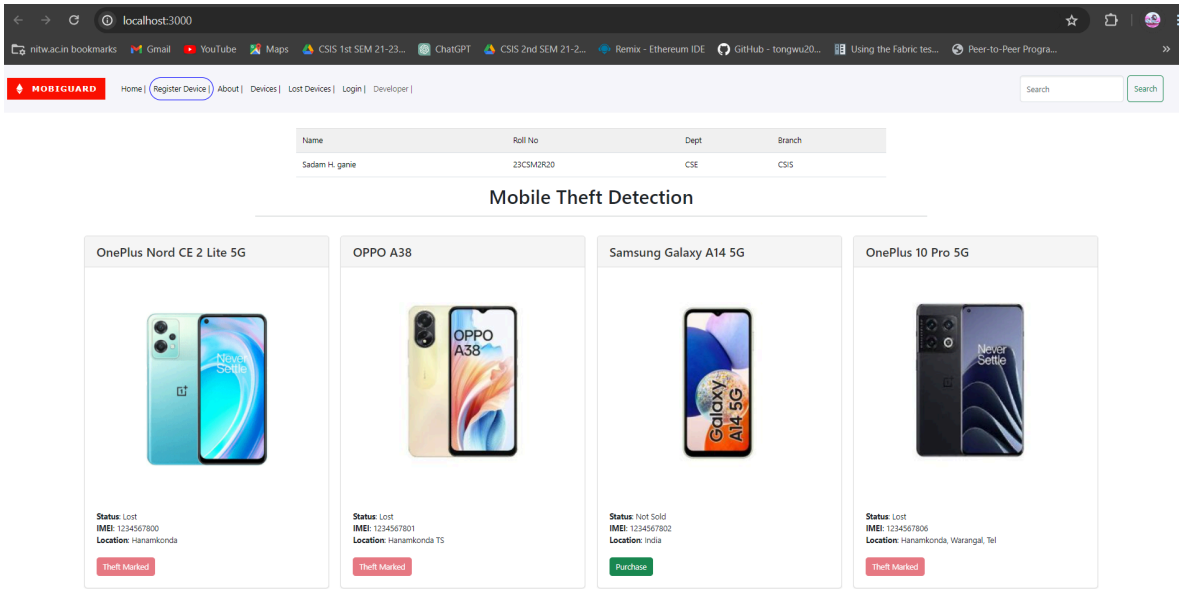

Figure 9: Index page. All the devices are listed with their status. Purchase button is enabled if the device is available for selling.

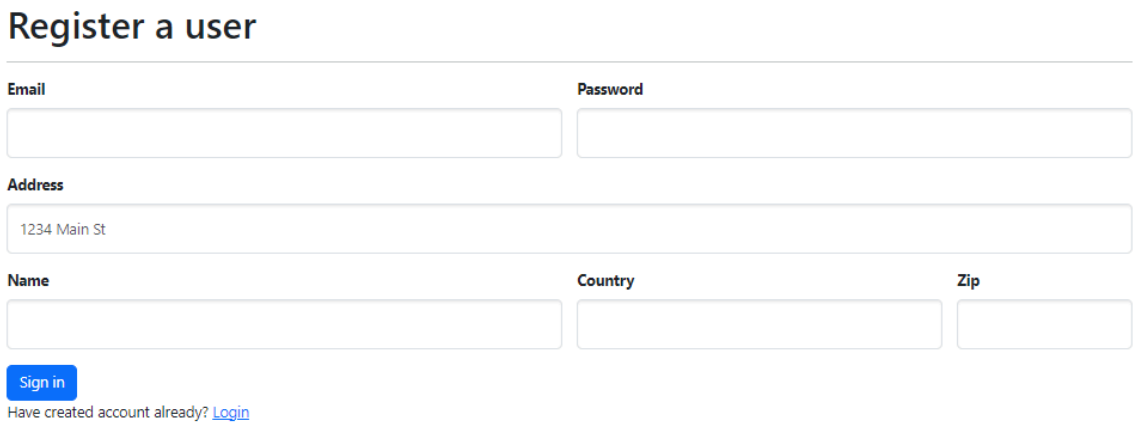

Figure 10: User registration page. Users can enter their details and register to avail facilities like purchasing a device.

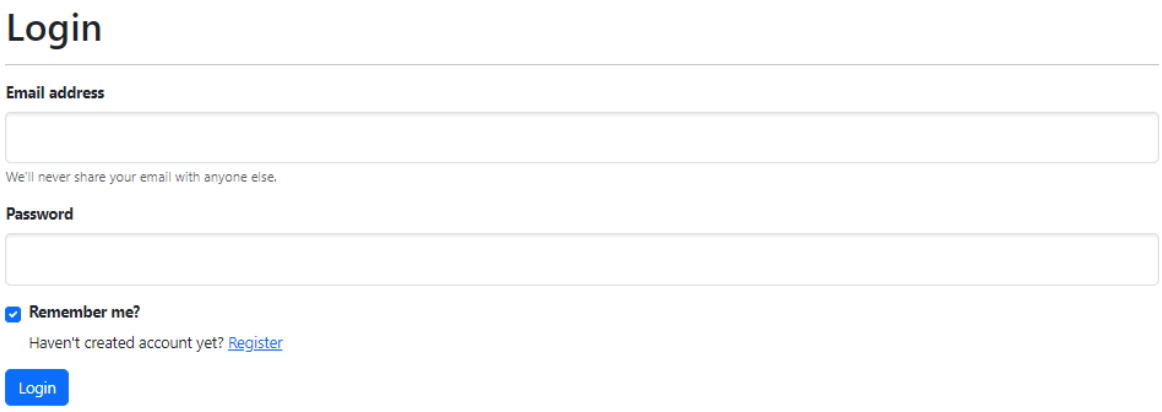

Figure 11: Login page. Registered users can login using their credentials.

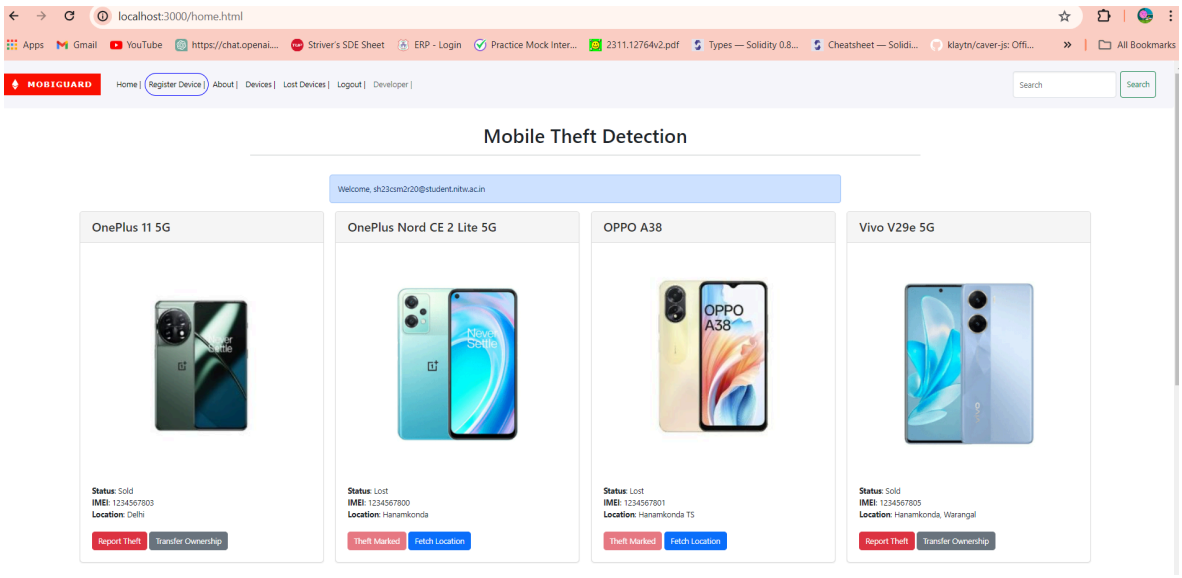

Figure 12: User dashboard. All the user owned devices are listed with different options like “ownership transfer”, “Mark theft”, “Fetch location” of lost device.

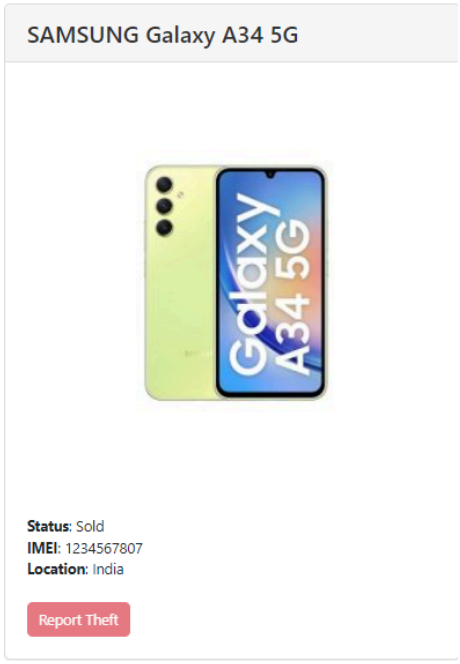

Figure 13: Purchased device. Purchased device listed on index page publicly with disabled button “Mark theft” because logged in user who is the owner of this device can utilize this feature on his user dashboard.

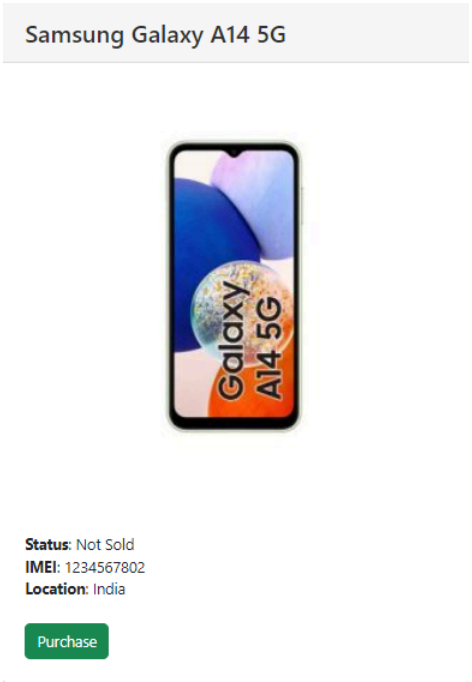

Figure 14: Unsold device. This device can be purchased by any authenticated logged in user. Note that the status of this device is “Not Sold”.

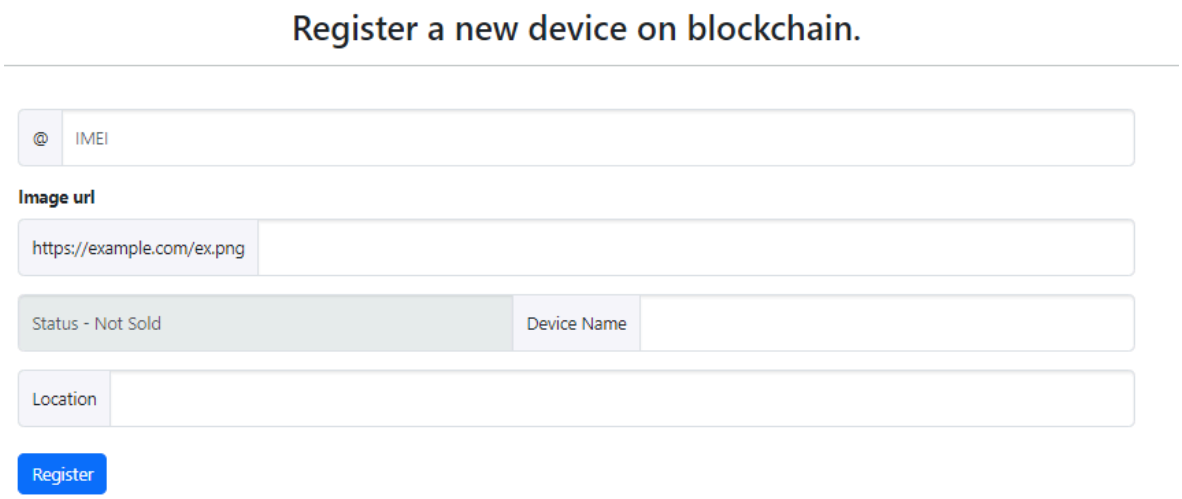

Figure 15: Device registration. This feature allows the manufacturers to register the mobile devices on the network.

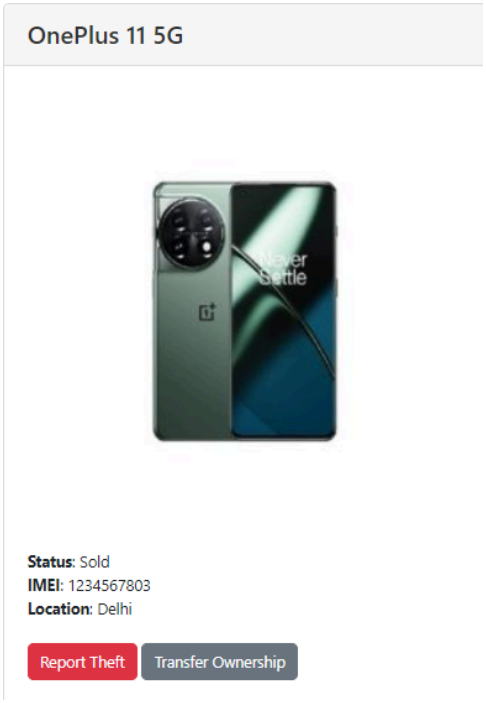

Figure 16: Device listed on user dashboard. Users can report the device theft or transfer ownership.

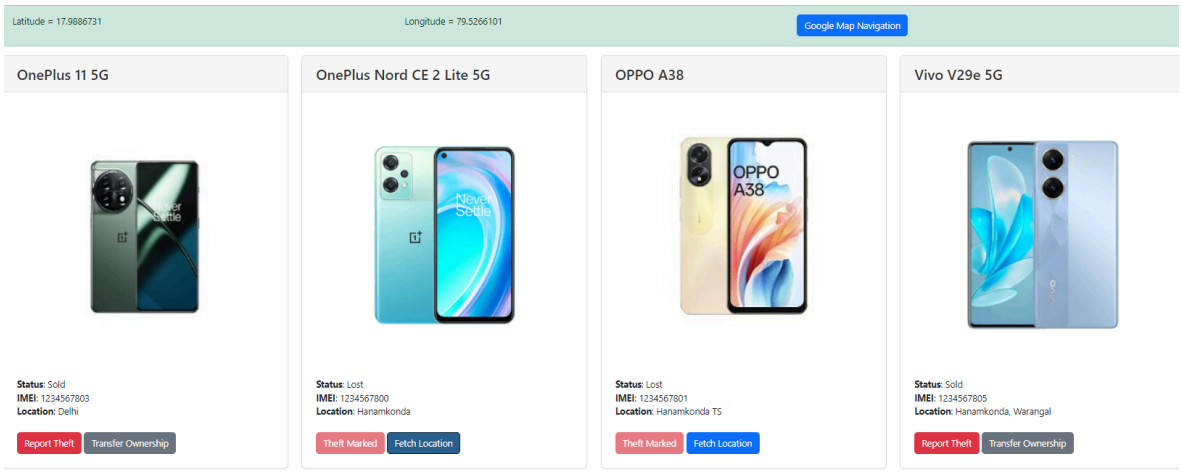

Figure 17: Fetch location. Users can fetch the location of “Theft” devices. Users can be guided via the google map navigation as shown in the figure.

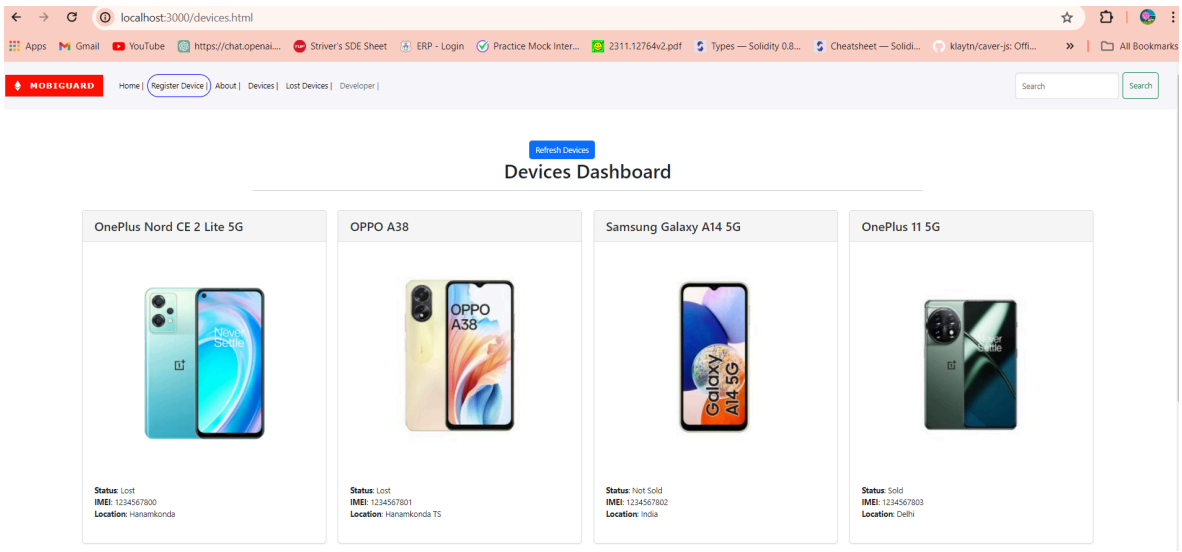

Figure 18: Device listing. This page lists all the devices irrespective of their status. It also displays the device information as shown in the figure.

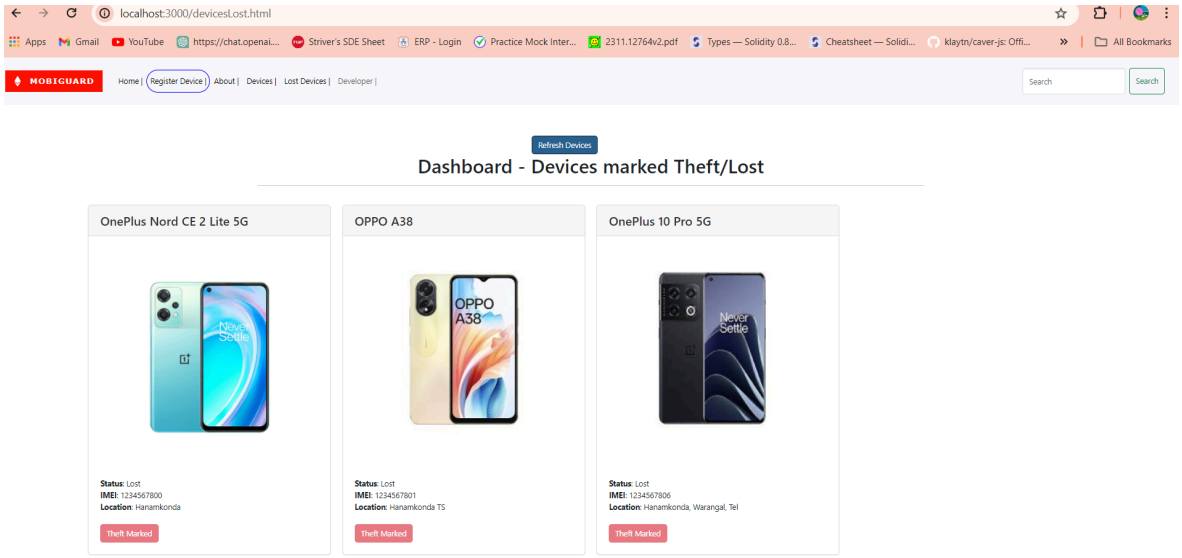

Figure 19: Lost devices. This page lists the devices which have been marked as theft/lost by their owners. Details like name, status, location of the device is displayed. This page guides the users to know about the lost devices to avoid unauthorized purchases.

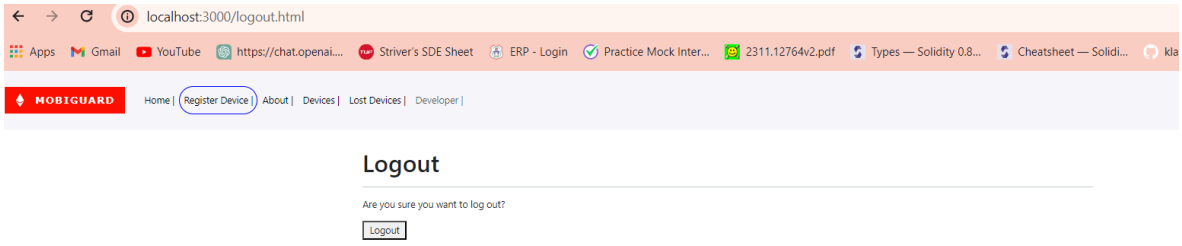

Figure 20: Logout page. This page asks the user for confirmation before logging him out.

5. Algorithms

Algorithm 1: Manufacturer's Device Registration Algorithm

Data: Device Details: IMEI
Result: Device Registration on Private Blockchain

```
if IMEI already exists then
    Reject registration;
end
else
    Register device on private blockchain;
end
```

Figure 21: Manufacturer's device registration algorithm. It outlines the logical process governing the "device registration" operation within our proposed system.

Algorithm 2: Purchase a Device Algorithm

Data: Device Status, Lost Status
Result: Device Purchase

```
if Device Status is "Not sold" and Lost Status is False then
    Update device status to "Sold";
    Update owner information;
    Operation successful;
end
else
    Reject operation;
end
```

Figure 22: Purchase a device algorithm. Algorithm 2 outlines the logical process governing the "device purchase" operation within our proposed system.

Algorithm 3: Ownership Transfer Algorithm

Data: Smartphone, User
Result: Device sold successfully

```
if state == "Sold" and seller is owner of device then
    Device owner info is updated;
    Device location is updated;
    Sell successful;
end
```

Figure 23: Ownership transfer algorithm. Algorithm 3 outlines the logical process governing the "device ownership transfer" operation within our proposed system. This operation is equivalent to selling a device by its owner to some other owner(Not

manufacturer).

Algorithm 4: Reporting Loss Algorithm

Data: Smartphone, User
Result: Device reported as lost or stolen
1 **if** *user == owner and device state == sold* **then**
2 | Update device status to "Lost";
3 | Monitor device location;
4 | Send notifications to owner of device;
5 **end**

Figure 24: Reporting loss algorithm. Algorithm 4 outlines the logical process governing the "mark theft" operation within our proposed system.

6. Conclusion

In conclusion, our blockchain-based mobile theft detection and event monitoring system represent a significant advancement in the realm of mobile security and anti-theft measures. By leveraging the power of blockchain technology, we have developed a robust and transparent platform that effectively addresses the challenges posed by mobile theft and loss.

Through the implementation of various modules, including device registration, user authentication, device purchase, and event monitoring, our system offers comprehensive protection for mobile devices and their users. The use of blockchain ensures the integrity and immutability of data, providing users with confidence in the security and reliability of the system.

Furthermore, our system incorporates innovative features such as real-time location tracking, ownership transfer, and dedicated dashboards for lost devices, enhancing user experience and facilitating prompt responses to security incidents.

Overall, our project demonstrates the immense potential of blockchain technology in mitigating the risks associated with mobile theft and loss. By providing a secure and transparent platform for managing mobile devices, we aim to contribute to a safer and more secure digital environment for users worldwide. Through further research and development, we envision our system evolving to become a standard solution for mobile security and anti-theft measures, offering peace of mind to mobile device users everywhere.

7. References

[1] E. J. Hom, "Mobile device security: startling statistics on data loss and data breaches." ChannelProNetwork, 2016.
[2] B. Henriquez, "Mobile theft and loss report - 2020/2021 edition." PREY Project, 2022.
[3] S. Fortis, "Samsung uses blockchain-based security for devices in its network." Cointelegraph, 2022.
[4] Huawei, "Huawei blockchain whitepaper." Huawei, 2018.

[5] Alotaibi, “In: Utilizing blockchain to overcome cyber security concerns in the internet of things: a review, in ieee,” Sensors journal, 2019.
[6] M. Privacy, “Detecting device theft in real time through walking pattern analysis,” IEEE Xplore Digital Library, 2020.
[7] Y. Gao, C. Zhou, and D. Shang, “A smart phone anti-theft solution based on locking card of mobile phone,” in 2011 International Conference on Computational and Information Sciences, 2011, pp. 971–974.
[8] A. Waheed, M. Riaz, and M. Y. Wani, “Antitheft mobile phone security system with the help of bios,” in 2017 International Symposium on Wireless Systems and Networks (ISWSN), 2017, pp. 1–6.
[9] G. Zhenge, Z. Haoyuan, W. Zhi, W. Yao, and D. Meiya, “Mobile phone anti-theft method based on mobile track and user characteristic,” in 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), 2019, pp. 28–32.
[10] A. U. S. Khan, M. N. Qureshi, and M. A. Qadeer, “Anti-theft application for android based devices,” in 2014 IEEE International Advance Computing Conference (IACC), 2014, pp. 365–369.
[11] IBM, “What is hyperledger fabric?” IBM Topics.
[12] A. G¨obel, “Using blockchain to prevent mobile phone theft,” Camelot, 2018.
[13] Chirag, “Blockchain: the technology revolutionizing mobile app security,” Appinventive, 2023.
[14] V. Shivam Dubey1 R, Eswari1A, “Mobile antitheft and privacy protection framework using blockchain,” Research Square, 2016.
[15] N. Q. Mohammed Abdul, Qadeer Mohammad, “Anti-theft application for android based devices,” PREY Project, 2022.
[16] Y. Yun, “The influence of blockchain technology on fraud and fake protection,” Cointelegraph,