A PRIVACY PRESERVING COMMUNICATION BETWEEN SMART VEHICLES

PROJECT REPORT

Submitted by

Sasirekha A	2018506109
Riyana Saffrin M	2018506095
Sathish Kumar Pillay R	2018506142

Under the supervision of

Dr. B. Lydia Elizabeth

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY
MADRAS INSTITUTE OF TECHNOLOGY CAMPUS ANNA UNIVERSITY, CHENNAI – 600044 OCTOBER 2020

ACKNOWLEDGEMENT

It is essential to mention the names of the people, whose guidance and encouragement made us accomplish this project. We express our thankfulness to our project guide Dr. B. Lydia Elizabeth, Department of Information Technology, MIT Campus, for providing invaluable support and assistance with encouragement which aided to complete this project. We are thankful to the panel members Dr. Radha Senthil Kumar, Dr. Uma Maheshwari and Mrs. Bala Gayathri Department of Information Technology, MIT Campus for their invaluable feedback in reviews. Our sincere thanks to Dr. Dhananjay Kumar, Head of the Department of Information Technology, MIT Campus for catering all our needs giving out limitless support throughout the project phase. We express our gratitude and sincere thanks to our respected Dean of MIT Campus, Dr. T. Thyagarajan, for providing excellent computing facilities throughout the project.

Sasirekha A **2018506109**

Riyana Saffrin M **2018506095**

Sathish Kumar Pillay R **2018506142**

Bonafide Certificate

Certified that this project report on “” is the bonafide work of “A Privacy Preserving Communication between Smart Vehicles” Sasirekha A (2018506109), Riyana Saffrin M (2018506095), Sathish Kumar Pillay R (2018506142) who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported herein does not form a part or full of any other work on the basis of which a degree or award was conferred on an earlier occasion on this to any other candidate.

SUPERVISOR

Dr. B. Lydia Elizebeth

SIGANTURE

Department of Information Technology
Madras Institute of Technology,
Anna University, Chennai – 600044.

Contents
Pg.No

A Privacy Preserving Communication between Smart Vehicles

Abstract

A Privacy Preserving Communication between Smart Vehicles is a most promising technology that aims to improve transport management system. In this infrastructure Smart Vehicles communicate wirelessly with other Smart Vehicles, Road Side Units and Trust Authority using Internet. However, the use of internet inherent vulnerabilities related to privacy (e.g., data poisoning attacks) and security issues (hacking data). People are less active in a network. To overcome all these challenges, A privacy preserving communication between smart vehicles is designed to provide both privacy and security. The proposed work provides security and privacy using blockchain and Machine Learning modules. Incentive mechanism is also included. Firstly, A Machine Learning module is designed to detect attacks in VANET. Secondly, a blockchain module is designed to securely transmit data. Thirdly, An Incentive mechanism is proposed to improve the participation rate in a network. The framework is validated and tested using CICIDS 2017 dataset.

Index Terms: Blockchain, Machine Learning, privacy-preserving, incentive mechanism, attacks detection.

1 Introduction

A Privacy Preserving Communication between smart vehicles is designed to facilitate improved road safety. The concept behind PPC is to improve the traffic management system by sharing information about the VANET to neighbor vehicles to avoid traffic, accidents etc.

Smart Vehicles (SV), Road Side Units (RSU) and Trusted Authority (TA) are the main components of PPC. The TA is responsible to authenticate every vehicle and also for transactions between vehicles. The Smart Vehicles are equipped with On-Board Unit for data storage and processing. The aim of Smart Vehicles is to provide efficient driving and reduces traffic fatalities. In addition to vehicle-to-vehicle communication, RSUs are positioned to disseminate data. PPC System provides two level of security using Blockchain and Machine Learning Algorithms. People hesitate to participate in a VANET because of privacy issues. And many attacks are also possible in VANET which are vulnerable to handle. And People lag to share timely information because of selfish attitude. To overcome all those aforementioned issues and to provide two level of security and privacy, blockchain and machine learning concepts are used.

Blockchain is a system of recording information in a way that makes it difficult or

impossible to change, hack or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer system on the blockchain. Blockchain is a decentralized database with an immutable hash. Private details of smart vehicles are going to be stored using blockchain to achieve security in VANET.

Machine Learning is a method of data analysis that automates analytical model building. All those possible attacks ex: DDoS attack, DoS attack, Web attack etc. are going to be detected using Machine Learning algorithms.

Incentive mechanism is included to improve the participation rate in a VANET by encouraging people to be active.

1.1 Scope of the Project

The scope of the project is to encourage and increase maximum participation in the network using incentive mechanism. Many vulnerable attacks are possible in VANET, those attacks are detected using machine learning models for safe driving and secure communication between smart vehicles using blockchain will also be achieved.

1.2 Motivation

Communication between smart vehicles in VANET reduces traffic and make driving more efficient. Meanwhile many attacks are possible in VANET and people hesitate to participate in sharing timely information because of selfish attitude and privacy issues. So the motive of the project is to overcome all those aforementioned issues.

1.3 Research Gap Identified

1. Cooperative Intelligent Transport System proposed in the base paper doesn't provides solution to improve the participation rate in VANET. We are trying to design a system that makes people to be more active in VANET by including incentive mechanism.
2. Fog computing is used in a base paper which is not cost efficient and secured. We are planning to use blockchain based storage system called IPFS, Inter Planetary File System designed to preserve and store data securely.

1.4 Dataset used in the base paper

1. CICIDS2017 Dataset
2. ToN-IoT Dataset

CICIDS2017 Dataset:

CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files). Also available is the extracted features definition.

ToN-IoT Dataset:

The TON_IoT datasets are new generations of Internet of Things (IoT) and Industrial IoT (IIoT) datasets for evaluating the fidelity and efficiency of different cybersecurity applications based on Artificial Intelligence (AI). The datasets have been called 'ToN_IoT' as they include heterogeneous data sources collected from Telemetry datasets of IoT and IIoT sensors. The datasets were collected from a realistic and large-scale network designed at the IoT Lab of the UNSW Canberra Cyber, the School of Engineering and Information technology (SEIT), UNSW Canberra @ the Australian Defence Force Academy (ADFA)

CICIDS 2017 Dataset Summary

S.No	File Name	Attack Names	Number of Instances
1	Monday-Working Hours	Benign	**529,918**
2	Tuesday-Working Hours	Benign	**432,074**
		SSH-Patator	**5,897**
		FTP-Patator	**7,938**
3	Wednesday-Working Hours	Benign	**440031**
		DoS attack	**252661**
4	Thursday-Working Hours-Morning-Web-attack	Benign	**168,186**
		Web Attack	**2180**
5	Thursday-Working-Hours-Afternoon-Infilteration	Benign	**288566**
		Infilteration	**36**
6	Friday-Working Hours-Morning	Benign	**189067**
		Bot	**1966**
7	Friday-Working-Hours-Afternoon-Portscan	Benign	**127537**
		PortScan	**158930**
8	Friday-Working-Hours-Afternoon-DDoS	Benign	**97718**
		DDoS	**128027**

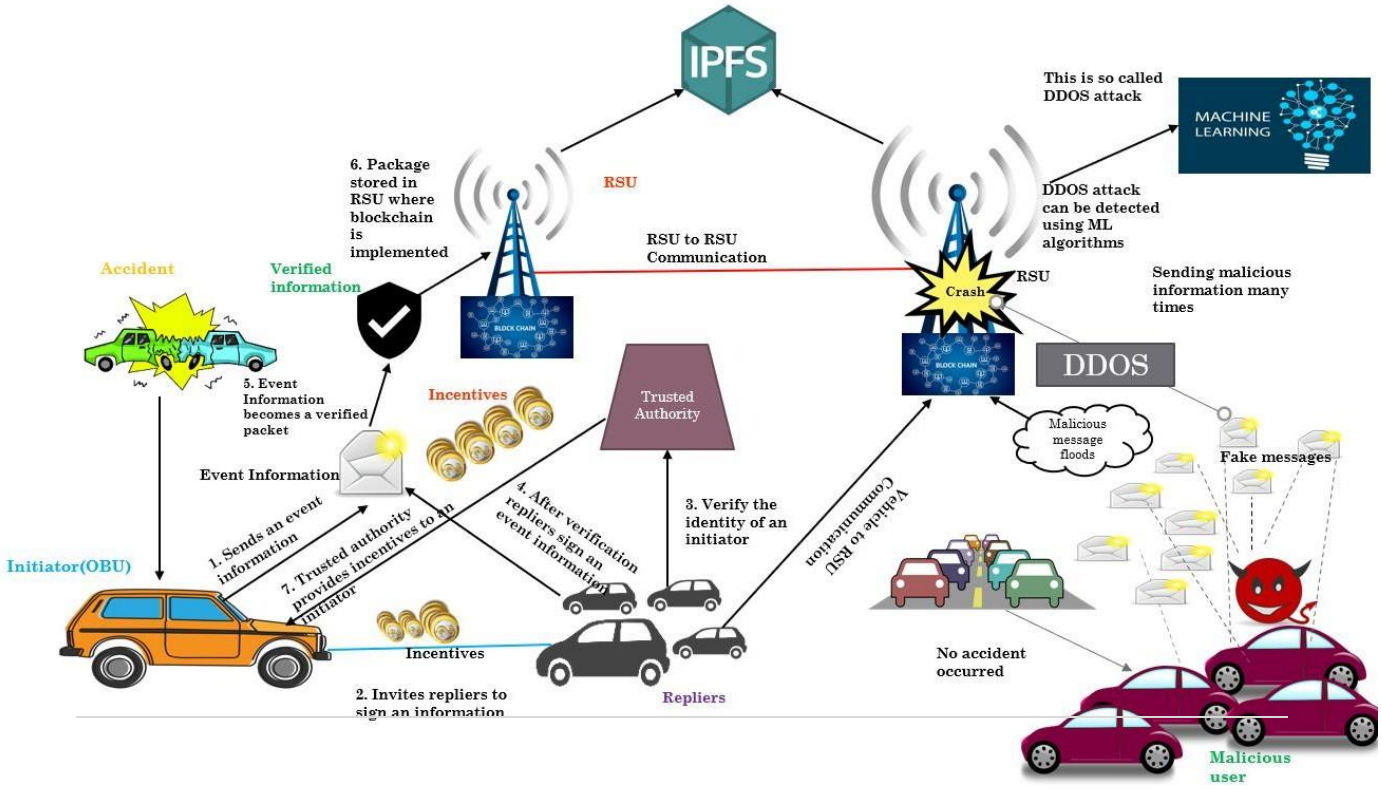
ToN-IoT Dataset Summary

Dataset	Normal	DDoS	Injection	Password	BackDoor	Ransomware	XSS	Scanning
Weather	**35000**	**5000**	**5000**	**5000**	**5000**	**2865**	**866**	**529**
Fridge	**35000**	**5000**	**5000**	**5000**	**5000**	**5000**	**2942**	**-**
Garage Door	**70000**	**10000**	**10000**	**10000**	**100000**	**5804**	**2312**	**1058**
GPS Tracker	**35000**	**5000**	**5000**	**5000**	**5000**	**2833**	**577**	**550**
IoT ModBus	**35000**	**-**	**5000**	**5000**	**5000**	**-**	**577**	**529**
IoT Motion Light	**70000**	**10000**	**10000**	**10000**	**10000**	**4528**	**898**	**3550**

1.5 Literature Survey

Title	Author	Year	Journal
BASE PAPER: **A Privacy Preserving based secure framework using blockchain enabled deep learning in cooperative intelligent transport system**	Randhir Kumar , Prabhat Kumar , Rakesh Tripathi, Govind P. Gupta Neeraj Kumar and Mohammad Mehedi Hassan	2021	IEEE Transaction on Intelligent Transport System
Credit Coin: A Privacy Preserving Blockchain based Incentive Announcement Network for Communications of Smart Vehicles	Jingzhong wang, Mengru Li, Yunhua He, Hong Li, KE Xiao and Chao Wang	2018	IEEE Transaction
Machine Learning Techniques to detect DDoS Attack on VANET System	Alia Mohammed Alrehan , Fahd Abdulsalam Alhaidari, Imam Abdulrahman.	2019	IEEE Transaction
A Blockchain based incentive provisioning scheme for traffic validation and information storage in VANET	Adia Khalid, Muhammad Sohaib Ifthikhar, A.S.Al.Mogren, Rabhiya Khalid	2020	Elsevier – Information Processing and Management

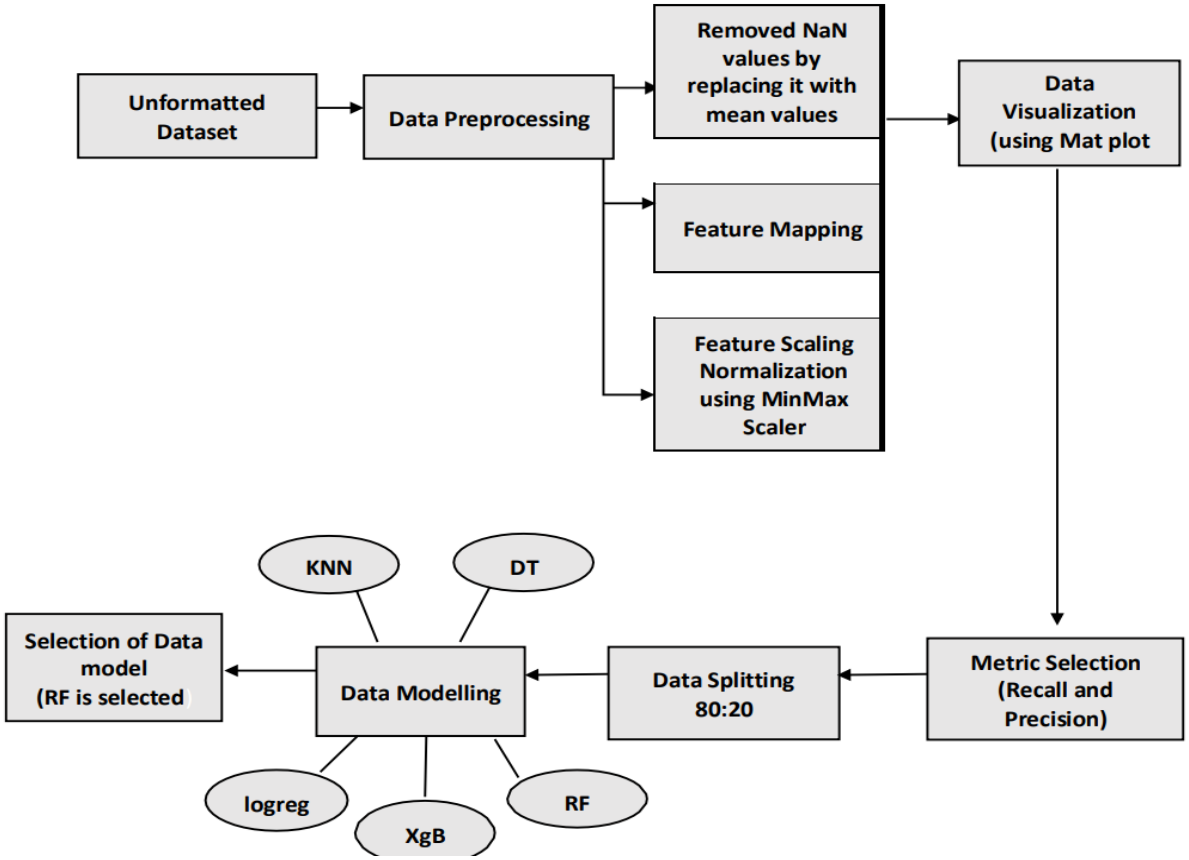
2 Overall Architecture



An Initiator is a vehicle who saw the particular event e.g. accident, sends an event information and invites repliers to vote for his particular event to make it a verified packet by giving some incentives from his own account. Repliers verifies the authentication of an initiator with Trust Authority and then sign a event initiated by an Initiator. Threshold vote count will be fixed. Once the number of votes crossed the threshold count, event information becomes a valid packet. Those valid packet are transmitted to neighboring vehicles and nearby RSUs. Blockchain is implemented in a RSU to store private details of an Initiator. An IPFS is used to store all verified packets. Once a packet becomes a verified packet, Trust Authority is going to provide some incentives to an initiator. Incentives provide by Trust Authority to an Initiator should be greater than incentives initialized by an initiator. Attacks in VANET are detected using Machine Learning Model and those malicious users are going to be removed from an environment.

3 Proposed Work

3.1 Block Diagram – Attacks Detection



3.2 Anonymous Message Passing System

In VANET, messages are shared anonymously to nearby vehicles using Ethereum blockchain. This improves the participation rate in VANET by providing security. To achieve this type of messaging, ganache and metamask connection should be obtained. An Initiator of a message needs to spend some ethers to share a message. 10 accounts with 100 free ethers are provided by ganache. Account from ganache should be imported in a metamask to obtain a connection.

3.3 Expected Outcome

Vehicles can share timely information anonymously. Event information are shared with other vehicles only when it becomes a valid packet. Incentive mechanism will be included to encourage more participation and various attacks in VANET are detected using machine learning models

4 Implementation of the Proposed Work

4.1 Data Preprocessing

CICIDS2017 is a dataset chosen to detect DDoS, DoS and Web attacks in VANET. The dataset is not in a proper and formatted manner. Data Processing is one of the important steps in Machine Learning. Many values are missing in this dataset. All the missing values are replaced by mean value of that particular column. Infinite floating values are removed. Feature mapping is done to map string values to numeric values. Feature Scaling is one the important step in Data Preprocessing. Feature Scaling is done using MinMax Scaler, a standard scaler to normalize large values between given range. Here large values are normalized between the range of 0 and 1. 80% of data is used for training and 20% of data is used for testing.

4.2 Attributes of the dataset

CICIDS2017 stands for Canadian Institute of Cybersecurity Intrusion Detection System 2017. This dataset contains details of benign and 7 common attacks.

DDoS attacks details are collected in the name of “Friday-WorkingHours-Afternoon-DDoS.pcap_ISCX.csv” file. This file contains details of 97,718 records of benign traffic and 128,027 records of DDoS traffics.

Web attack details are collected in the name of “Thursday-WorkingHours-Afternoon-WebAttack.pcap.csv” file. This file contains details of 168186 records of benign, 1507 records of Web Attack – Brute Force, 652 records of XSS and 21 records of SQL Injection.

DoS Attack details are collected in the name of “Wednesday-WorkingHours-DosAttack.pcap_ISCX.csv” file. This file contains details of Benign 440,031, DoS Hulk 231,073, DoS GoldenEye, 10,293 DoS Slowloris, 5,796 DoS Slowhttptest ,5,499 and Heartbleed 11

4.3 Head of the dataset

Dataset for DDoS Attack

	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	Bwd Packet Length Max	Bwd Packet Length Min	Bwd Packet Length Mean	Bwd Packet Length Std	Flow Bytes/s	Flow Packets/s	Flow IAT Mean	Flow IAT Std	Flow IAT Max	Flow IAT Min
0	54865	3	2	0	12	0	6	6	6.0	0.0	0	0	0.0	0.0	4.000000e+06	666666.66670	3.0	0.0	3	3
1	55054	109	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	1.100917e+05	18348.62385	109.0	0.0	109	109
2	55055	52	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	2.307692e+05	38461.53846	52.0	0.0	52	52
3	46236	34	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	3.529412e+05	58823.52941	34.0	0.0	34	34
4	54863	3	2	0	12	0	6	6	6.0	0.0	0	0	0.0	0.0	4.000000e+06	666666.66670	3.0	0.0	3	3
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
225740	61374	61	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	1.967213e+05	32786.88525	61.0	0.0	61	61
225741	61378	72	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	1.666667e+05	27777.77778	72.0	0.0	72	72
225742	61375	75	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	1.600000e+05	26666.66667	75.0	0.0	75	75
225743	61323	48	2	0	12	0	6	6	6.0	0.0	0	0	0.0	0.0	2.500000e+05	41666.66667	48.0	0.0	48	48
225744	61326	68	1	1	6	6	6	6	6.0	0.0	6	6	6.0	0.0	1.764706e+05	29411.76471	68.0	0.0	68	68

225745 rows × 79 columns

Dataset for Web Attack

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	Bwd Packet Length Max	Bwd Packet Length Min	Bwd Packet Length Mean
192.168.10.50	33898.0	192.168.10.3	389.0	6.0	6/7/2017 8:59	113095465.0	48.0	24.0	9668.0	10012.0	403.0	0.0	201.416667	203.548293	923.0	316.0	417.166667
192.168.10.50	33904.0	192.168.10.3	389.0	6.0	6/7/2017 8:59	113473706.0	68.0	40.0	11364.0	12718.0	403.0	0.0	167.117647	171.919413	1139.0	126.0	317.950000
8.6.0.1	0.0	8.0.6.4	0.0	0.0	6/7/2017 8:59	119945515.0	150.0	0.0	0.0	0.0	0.0	0.0	0.000000	0.000000	0.0	0.0	0.000000
192.168.10.14	59135.0	65.55.44.109	443.0	6.0	6/7/2017 8:59	60261928.0	9.0	7.0	2330.0	4221.0	1093.0	0.0	258.888889	409.702162	1460.0	0.0	603.000000
192.168.10.14	59555.0	192.168.10.3	53.0	17.0	6/7/2017 8:59	269.0	2.0	2.0	102.0	322.0	51.0	51.0	51.000000	0.000000	161.0	161.0	161.000000

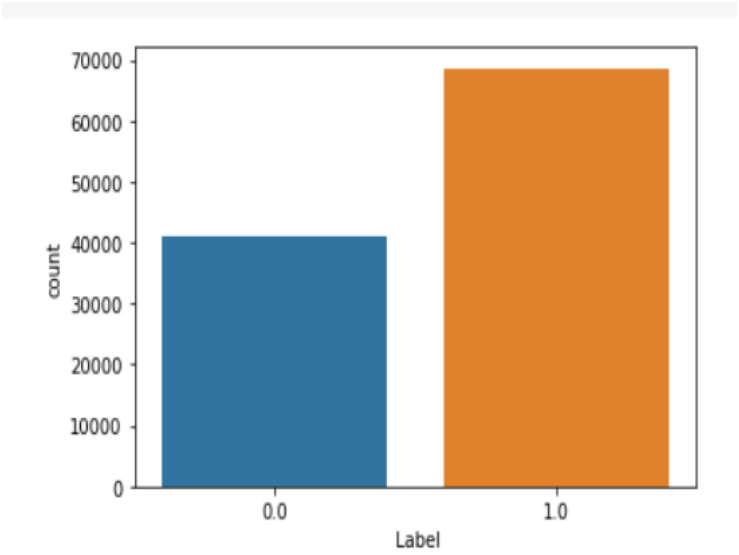
Dataset for DoS Attack

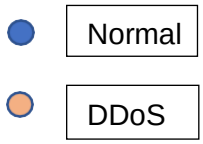
	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	Bwd Packet Length Max	Bwd Packet Length Min	Bwd Packet Length Mean	Bwd Packet Length Std	Flow Bytes/s	Flow Packets/s	Flow IAT Mean	F
0	80	38308	1	1	6	6	6	6	6.000000	0.000000	6	6	6.000000	0.000000	3.132505e+02	52.208416	38308.000000	
1	389	479	11	5	172	326	79	0	15.636364	31.449238	163	0	65.200000	89.278777	1.039666e+06	33402.922760	31.933333	
2	88	1095	10	6	3150	3150	1575	0	315.000000	632.561635	1575	0	525.000000	813.326503	5.753425e+06	14611.872150	73.000000	
3	389	15206	17	12	3452	6660	1313	0	203.058824	425.778474	3069	0	555.000000	977.480342	6.650007e+05	1907.141918	543.071429	
4	88	1092	9	6	3150	3152	1575	0	350.000000	694.509719	1576	0	525.333333	813.842901	5.771062e+06	13736.263740	78.000000	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	
2698	53	32215	4	2	112	152	28	28	28.000000	0.000000	76	76	76.000000	0.000000	8.194940e+03	186.248642	6443.000000	
2699	53	324	2	2	84	362	42	42	42.000000	0.000000	181	181	181.000000	0.000000	1.376543e+06	12345.679010	108.000000	
2700	58030	82	2	1	31	6	31	0	15.500000	21.920310	6	6	6.000000	0.000000	4.512195e+05	36585.365850	41.000000	
2701	53	1048635	6	2	192	256	32	32	32.000000	0.000000	128	128	128.000000	0.000000	4.272221e+02	7.628965	149805.000000	3
2702	53	94939	4	2	188	226	47	47	47.000000	0.000000	113	113	113.000000	0.000000	4.360695e+03	63.198475	18987.800000	

703 rows × 79 columns

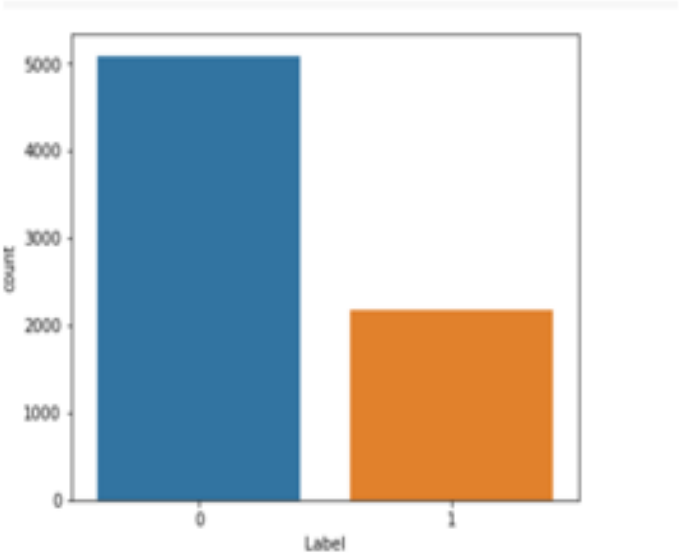
4.4 Data Visualization

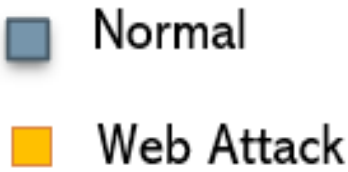
DDoS Attack



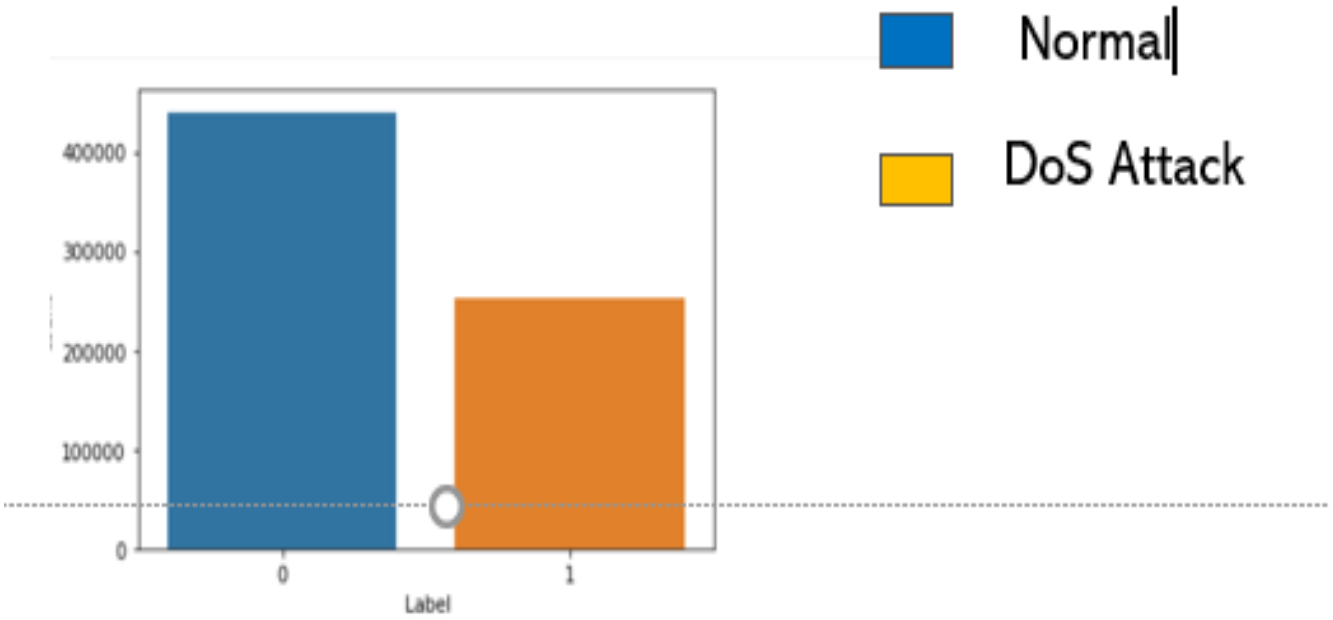


Web Attack





DoS Attack:



4.5 Under Sampling against Unbalance

Under sampling is the method of correcting imbalances in classes. Data set used to detect Web attack is unbalanced. The dataset contains 168186 benign records and 2180 records of web attack. So under sampling is used to correct class imbalances. Most of the BENIGN records are removed to form a balanced dataset

4.6 Hyper Parameter Tuning

Hyper parameter tuning is used to tune the parameters of random forest algorithm to detect web attack. Hyperparameter tuning is choosing a set of optimal hyperparameters for a learning algorithm. A hyperparameter is a model argument whose value is set before the learning process begins. The key to machine learning algorithms is hyperparameter tuning.

4.7 Data Model

4.7.1 Logistic Regression

```
from sklearn.linear_model import
LogisticRegression logreg =
LogisticRegression(random_state = 42)
logreg.fit(X_train, Y_train)
```

4.7.2 K-Nearest Neighbor

```
from sklearn.neighbors import KNeighborsClassifier
knn = KNeighborsClassifier(n_neighbors = 5, metric =
'euclidean', p = 2) knn.fit(X_train, Y_train)
```

4.7.3 Decision Tree

```
from sklearn.tree import DecisionTreeClassifier
dectree = DecisionTreeClassifier(criterion = 'entropy', random_state
= 42) dectree.fit(X_train, Y_train)
```

4.7.4 Random Forest

```
from sklearn.ensemble import RandomForestClassifier

ranfor= RandomForestClassifier(n_estimators = 10, criterion = 'entropy',
random_state = 42) ranfor.fit(X_train, Y_train)
```

4.7.5 XgBoost

```
from xgboost import
XGBClassifier import time
xgb =
XGBClassifier(n_estimators=200,scale_pos_weight=5,min_child_weight=1,max_depth=2,ra
ndom_st ate=5)
training_start =
time.perf_counter()
xgb.fit(X_train, Y_train)
```

4.8 Model Selection

The aim to reduce the false positive and false negative rate. So recall and precision are chosen as a metric to calculate the performance of a model. **Random forest** gave more recall and precision score as well as less false positive and false negative rate. So Random Forest is chosen.

4.8.1 DDoS Attack Detection

RECALL SCORE:
Recall score for RF
:0.9985419704228286 Recall score for
Logreg :0.9992449489689648 Recall
score for KNN :0.9985680066652781
Recall score for Decision Tree
:0.9985159341803791 Recall score for XgBoost
:0.9991408039991668

PRECISION SCORE:
Precision score for RF
:0.9998435789144376 Precision score for
Logreg :0.9339092347000851 Precision
score for KNN :0.9997653928366613
Precision score for Decision Tree
:0.9998435748364054 Precision score for XgBoost
:0.9977899115964639

4.8.2 Web Attack Detection

RECALL SCORE:
Recall score for RF :0.9729729
Recall score for Logreg :0.9592
Recall score for KNN :0.94856
Recall score for Decision Tree :0.96851
Recall score for XgBoost :0.9598

PRECISION SCORE:
Precision score for RF
:0.9668435789144376 Precision score for Logreg :0.9339092347000851 Precision score for KNN :0.9197653928366613
Precision score for Decision Tree :0.9098435748364054 Precision score for XgBoost :0.9577899115964639

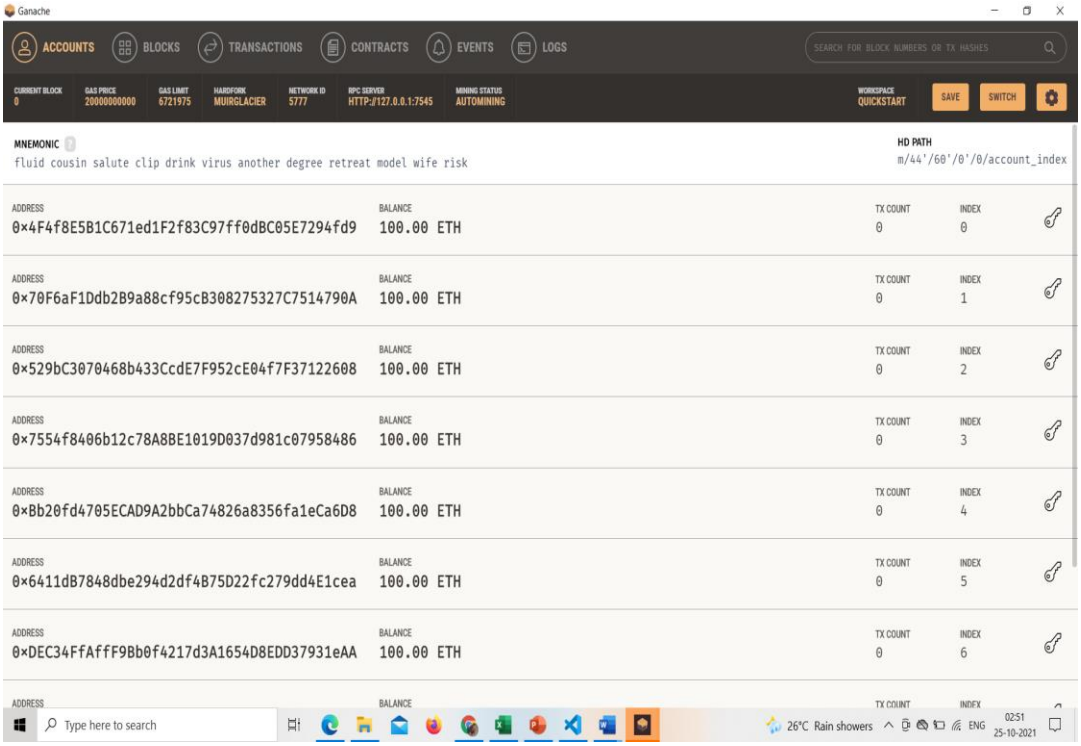
4.8.3 DoS Attack Detection

RECALL SCORE:
Recall score for RF :0.9953
Recall score for Logreg :0.6366
Recall score for KNN :0.9984
Recall score for Decision Tree :0.99.54
Recall score for XgBoost :0.9997

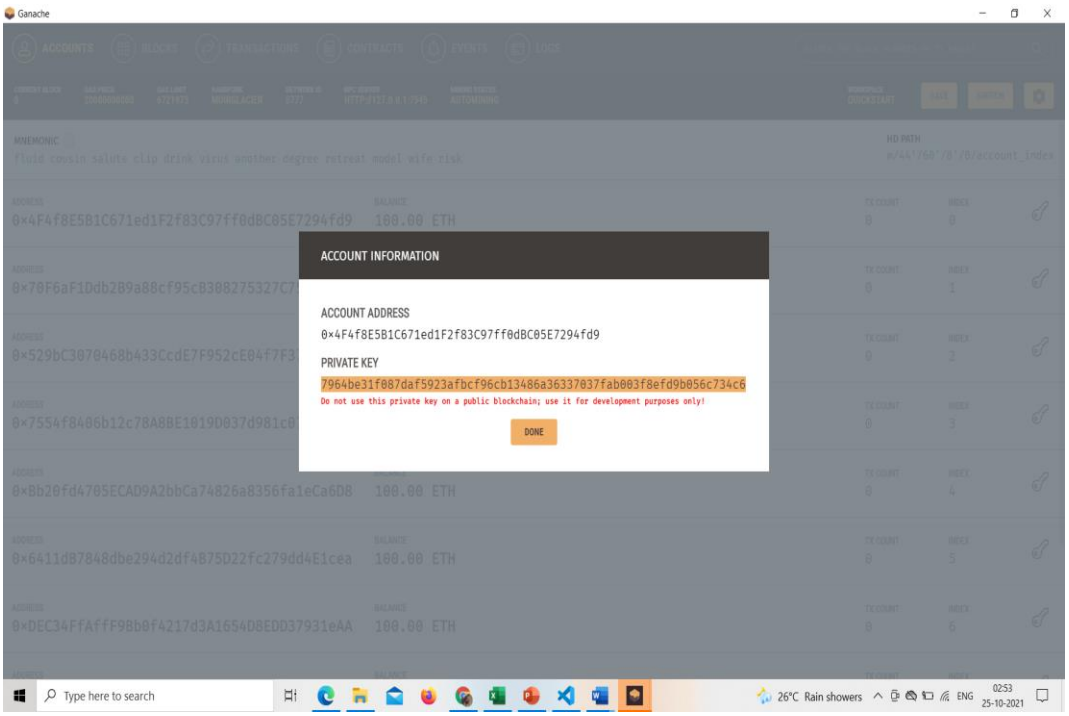
PRECISION SCORE:
Precision score for RF :0.9558
Precision score for Logreg :0.9210
Precision score for KNN :0.9556
Precision score for Decision Tree :0.9556
Precision score for XgBoost :0.9262

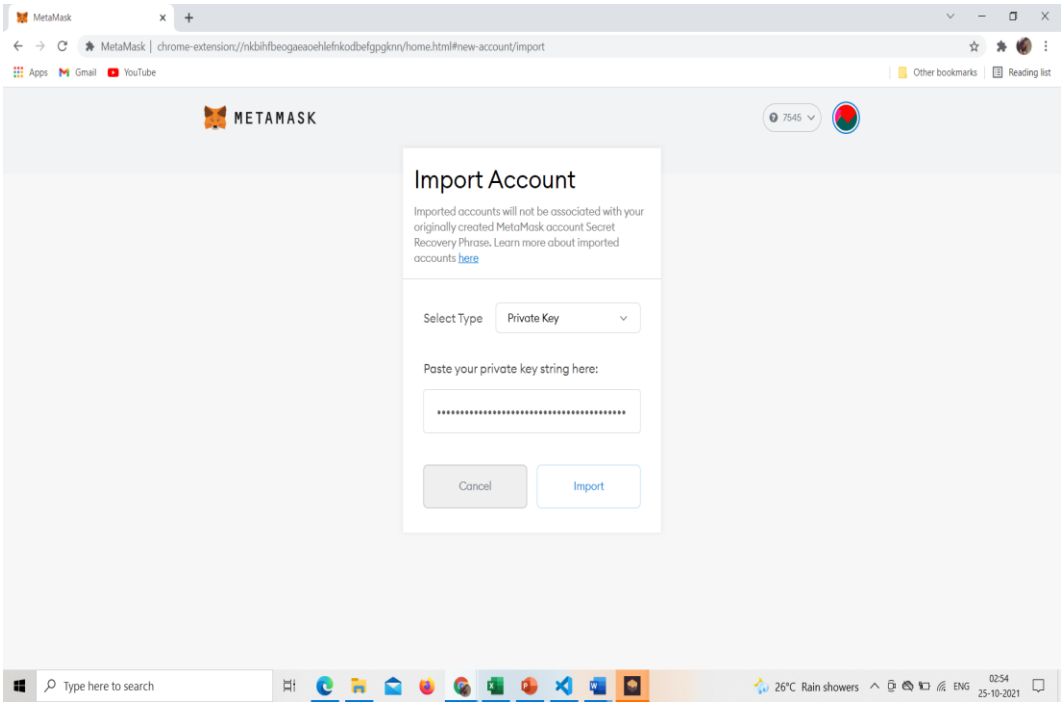
4.9 Ganache and Metamask Connection

Ganache:

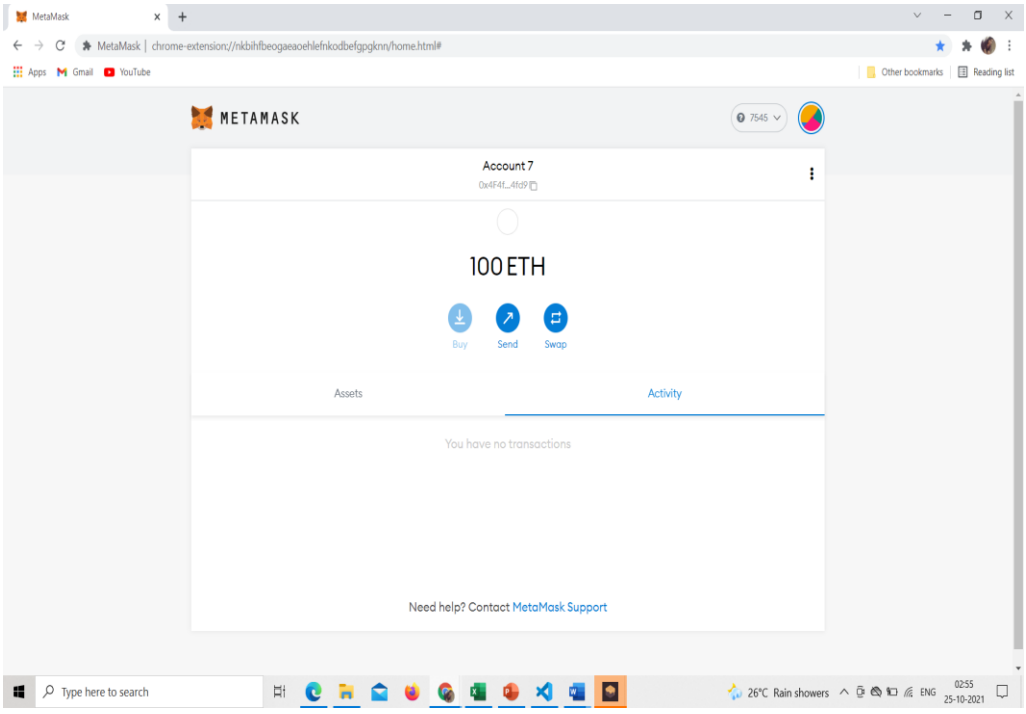


Import Accounts

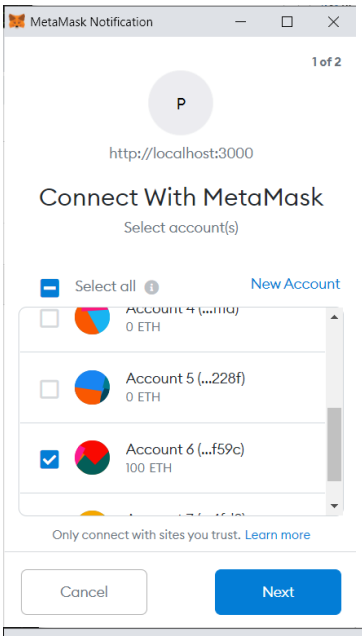


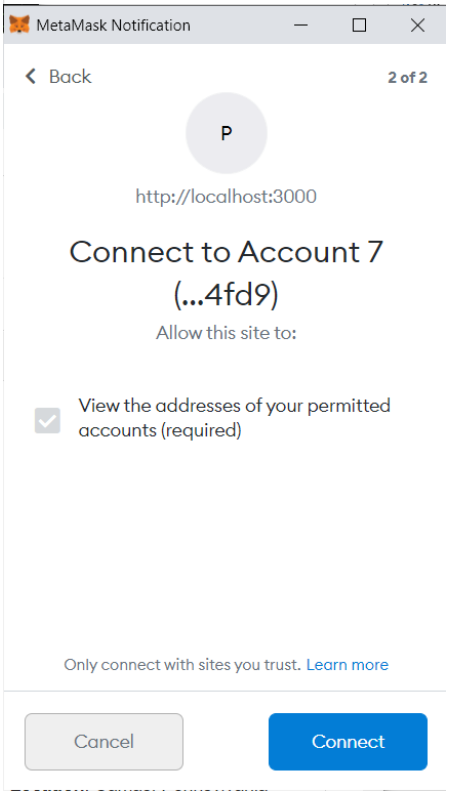


Account Imported Successfully

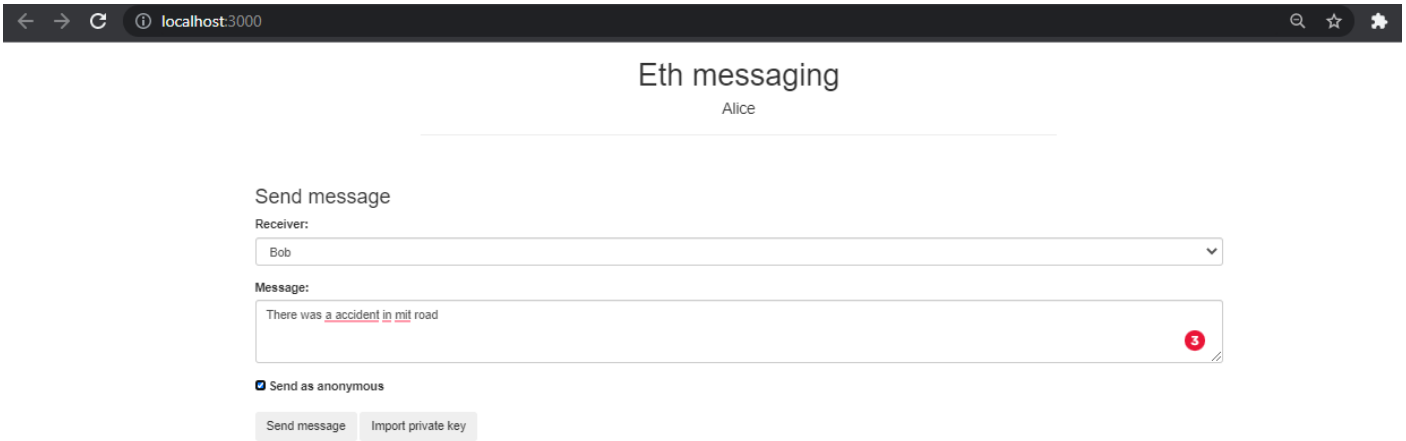


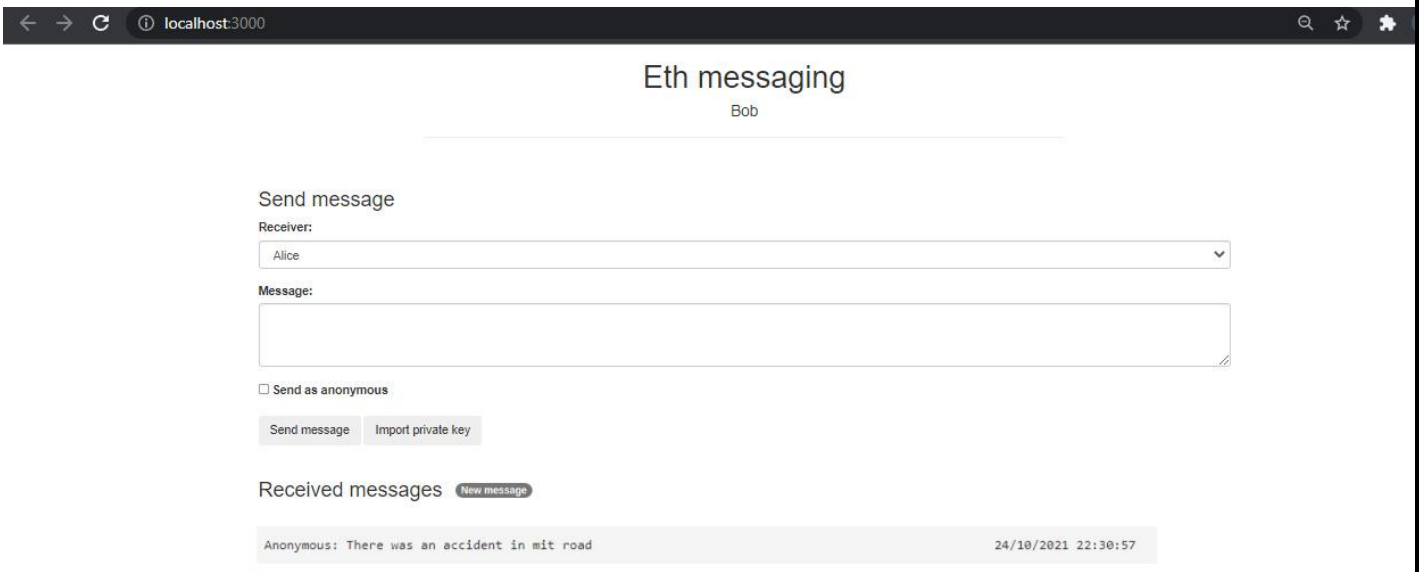
Localhost Connection with Metamask





4.10 Anonymous Communication Using Ethereum


localhost:3000
Eth messaging
Alice
Send message
Receiver:
Bob
Message:
There was a accident in mit road
3
Send as anonymous
Send message
Import private key
Received messages


localhost:3000
Eth messaging
Bob
Send message
Receiver:
Alice
Message:
Send as anonymous
Send message
Import private key
Received messages
New message
Anonymous: There was an accident in mit road
24/10/2021 22:30:57

5 Project Baseline Requirements

5.1 Software Requirements

- Google Collaboratory
- Visual Studio Code (1.60)
- Ganache – Ethereum (v7.0.0)
- Meta Mask (10.1.1)
- Solidity Language version 6
- Python Language (Python3)
- SUMO – Online Simulator
- IPFS version 0.4.19

5.2 Hardware Requirements

- Processor: Intel Core i5
- Operating System: Windows 10
- Memory: 2GB or above

5 Reference

[1] Kang, Jiawen Zehui Xiong,Duist Nivato, Dongdong Ye, DonIn Kim and Jun Zhao." Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract Theory." IEEE Transactions on Vehicular Technology (2019)

[2] Y. A. O. Yu, L. E. I. Guo, Y. E. Liu, J. Zheng, and Y. U. E. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," IEEE Access, vol. 6, pp. 44570–44579, 2018.

[3] A. Haydari, "Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems," no. September, 2018.

[4] Wang, Yuntao, Zhou Su, and Ning Zhang. "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network." IEEE Transactions on Industrial Informatics 15, no. 6 (2019): 3620-3631.

[5] Lu, Zhaojun, Qian Wang, Gang Qu, Haichun Zhang, and Zhenglin Liu. "A blockchain-based privacy-preserving authentication scheme for vanets." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 27, no. 12 (2019): 2792-2801