IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Decentralized block chain based trust management protocol for the internet of things

Dr J. Sarada[1] , L. Ramesh[2], D. Lakshmi Narayana[3]

[1] Associate Professor, Department of Computer Applications , Chadalawada Ramanamma Engineering College Tirupati , Andhra Pradhesh, India.

[2,3] Student, Department of Computer Applications, Chadalawada Ramanamma Engineering College Renigunta Rd, Tirupati, Andhra Pradesh, India

Abstract- The Internet of Things (IoT) is a network that integrates a variety of heterogeneous nodes, such as connected devices (sensors, robots, and smart phones ...), connected cars, smart homes, etc. These smart objects communicate and collaborate in distributed and dynamic environments that are facing several security challenges. Trust management is one of the most important challenges in IoT. Existing trust management solutions do not meet the new requirements of IoT such as heterogeneity, mobility, and scalability. In this article, we propose a hierarchical and scalable blockchain-based trust management protocol with mobility support in massively distributed IoT systems. In our protocol, mobile smart objects disseminate trust information on service providers to the blockchain. Thus, all the objects will have a global view on each service provider in the architecture, which speeds up the trust evaluation process. In addition, our protocol is resilient against the most known malicious attacks such as bad-mouthing , ballot-stuffing , and cooperative attacks . We confirm the efficiency of our proposal through theoretical analysis and extensive simulations. Finally, we show that it outperforms existing solutions, especially in terms of scalability, mobility support, communication, and computation costs.

Keywords— Internet of Things, Trust management, Blockchain, Protocols, Cloud computing, Computer architecture, Peer-to-peer computing.

I. INTRODUCTION

IoT can be viewed as a service centric architecture where each device, can request services from other devices and it may also provide services to other devices (service provider). The service centric based IoT applications are facing several security challenges such as trust management. Indeed, IoT service providers can behave maliciously for the purpose of promoting itself and defame the honest service providers. Hence, they can trick IoT devices to request services from them instead of the honest onces and monopolize many provided services by performing discriminatory, bad-mouthing and ballot-stuffing attacks. Therefore, it is clear that a trust management protocol which evaluates the trustworthiness of IoT service providers, in a scalable and efficient way, is required.

Besides, in some cases, an IoT device needs to assess the trust level of a new encountered service provider in a fast way, without necessarily performing a lot of exchanges. Existing trust management solutions do not efficienlty deal with these cases. In fact, without any previous exchange, a new encountered service provider is assumed to have a predefined initial trust value,

whereas it could be malicious. Other clustering and centralized based trust management approaches have been investigated in several worksin order to enhance the process of trust computation and optimization of IoT resources. Although these approaches allow constrained IoT devices to efficiently assess trustworthiness of each other, these devices only have access to trust data in their own cluster (no global view of trustworthiness). Furthermore, these

protocols usually assume that the cluster heads are pre-trusted nodes. However, such assumption is not practical in most IoT applications.

Hence, this brings us back to an important question: how can we ensure a fully distributed and scalable trust management protocol with mobility support, in which IoT devices can evaluate trustworthiness of any service provider in the Internet, without the presence of any pre-trusted entity.

II. RELATEDWORKS

1.Title : Hierarchical trust management for wireless sensor networks and its applications to trustbased routing and intrusion detection

Author : R Chen and M Zhang

Description : propose a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a novel probability model, describe a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield "ground truth" node status. This serves as a basis for validating our protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of our hierarchical trust management protocol, apply it to trust-based geographic routing and trust-based intrusion detection. For each application, identify the best trust composition and formation to maximize application performance. Our results indicate that trust-based geographic routing approaches the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, we discover that there exists an optimal trust threshold for minimizing false positives and false negatives.

2. Title: Trust management for encounter-based routing in delay tolerant networks

Author: R Chen

Description: propose and analyze a class of trust management protocols for encounter-based routing in delay tolerant networks (DTNs). The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only quality-of-service (QoS) trust properties (connectivity) but also social trust properties (honesty and unselfishness) to evaluate other nodes encountered. Two versions of trust management protocols are considered: an equal-weight QoS and social trust management protocol (called trust-based routing) and a QoS only trust management protocol (called connectivity-based routing). By utilizing a stochastic Petri net model describing a DTN behavior, analyze the performance characteristics of these two routing protocols in terms of message delivery ratio, latency, and message overhead. also perform a comparative performance analysis with epidemic routing for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that trust-based routing approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance in message delay of epidemic routing, especially as the percentage of selfish and malicious nodes present in the DTN system increases.

3. Title : Trust management for SOA-based IoT and its application to service composition

Author: F Buo and J Gio

Description: A future Internet of Things (IoT) system will connect the physical world into cyberspace everywhere and everything via billions of smart objects. On the one hand, IoT devices are physically connected via communication networks. The service oriented architecture (SOA) can provide interoperability among heterogeneous IoT devices in physical networks. On the other hand, IoT devices are virtually connected via social networks. In this paper propose adaptive and scalable trust management to support service composition applications in SOA based IoT systems. develop a technique based on distributed collaborative filtering to select feedback using similarity rating of friendship, social contact, and community of interest relationships as the filter. Further develop a novel adaptive filtering technique to determine the best way to combine direct trust and indirect trust dynamically to minimize convergence time and trust estimation bias in the presence of malicious nodes performing opportunistic service and collusion attacks. For scalability, consider a design by which a capacity-limited node only keeps trust information of a subset of nodes of interest and performs minimum computation to update trust.

In Existing,proposed a 3-tier hierarchical architecture based on cloudlets to disseminate trust information to a central cloud. Their architecture allows IoT devices to report trust information and also query trustworthiness of other devices directly from the local cloudlets. However, the proposed architecture always refers to the central cloud which is responsible for the dissemination of trustworthiness information gathered from one cloudlet to the other cloudlets which can involve latency issues. Moreover, their trust model is still limited, since the distributed cloudlets are assumed to be honest in the architecture and they maintainonly trust data in their geographical area. In another approach, proposed a trust management model based on fuzzy reputation concept for IoT. However, they considered only some specific WSN applications where nodes can establish limited trust relationships with other nodes. Compared to WSN nodes, IoT devices are internet enabled and can establish complex relationships with other IoT devices and owners.

Disadvantages of existing system

→The system is not implemented BC-Trust which is a real time assessment process, which provides trust information about any service provider.

→The system is not implemented a Block generation and consensus protocol

III. PROPOSED SYSTEM ARCHITECTURE

In proposed system ,present a new scalable trust management solution, named **BC-Trust**, to address the aforementioned limitations. Our solution is based on blockchain technology and fog computing paradigm, and allows highly mobile IoT devices to accurately assess and share trust recommendations about other devices in a scalable way without referring to any pre-trusted entity.

The contributions of this project are as follows :

1. The mobility support: given the nature of our architecture which is geographically distributed as well as the ubiquitous nature of our architecture, mobile devices could assess trustworthiness of service providers in real time after few message exchanges.

2. The scalability: our architecture scales very well and deals efficiently with tremendous number of IoT devices. Indeed, IoT devices do not need to manage and exchange trust information with each other, instead the whole process is devoted to fog nodes in a distributed way.

3. A global view of trust data: in our architecture, trust data is disseminated and duplicated into the blockchain, maintained by decentralized and powerful fog nodesthat make it accessible from anywhere.

4. The optimization of IoT devices resources: in our architecture, data storage and trust computation are offloaded to powerful fog nodes. Therefore, IoT devices optimize their storage and computation resources.

5. Fine-grained based service: IoT objects get recommendations about service providers not just according to the service they want, but also according to a set of requirements that these providers are able to satisfy.

6. Resiliency against cooperative attacks: our proposed approach deals efficiently with cooperative bad-mouthing and ballot-stuffing attacks thanks to the history of the recommendations maintained in the blockchain.

ADVANTAGES OF PROPOSED SYSTEM

➢The optimization of IoT devices resources: in our architecture, data storage and trust computation are offloaded to powerful fog nodes. Therefore, IoT devices optimize their storage and computation resources.

➢Resiliency against cooperative attacks: our proposed approach deals efficiently with cooperative bad-mouthing and ballot-stuffing attacks thanks to the history of the recommendations maintained in the blockchain.

In this Proposed System, There are Four Modules. They are:

➢Data Owner

➢IOT Server

➢Data Receiver

➢Authority

1.IOT Server:

In this module, The IOT Server maintained their data in server. he should login . after login with valid details he can perform some operation like view al data owner file block sin Encrypt format with Id, owner name, Access

details, file blocks with its sign, view all content and secret key Attackers with date and IP address, view all owner secret key and end key request, result with date and time .

2. Data Owner

In this module, the Data Owner maintained their data in server. and he should register and login. After login he can perform some operations view Profile, enter the file name generate encrypt key from authority and view the response without entering file name and owner name, check the encrypt key request and secret key request and then browse the file and give access to researchers power grid staff, govt staff others, view all files and give update and delete option, view all upload file with access permission, view all files verify any file and recover, Enter file name and get secret key permission from AA and view response without entering file name.

3. Authority

In this module, Authority maintained their data in server, in this Authority login with valid details and then perform some operation like View all data owner and authorize, view all end user and authorize, view all encrypt key permission request, view all secret key permission and generate using RSA, view decrypt key request from user and give permission request secret key from user and give permission.

4. Data Receiver

In this module, the Data Receiver maintained their data in server, he can perform some operation like register with researchers power grid staffs, govt staff, othes and logins with valid details, view profile, view all authorize data, search data on only authorize using content key word and view its details, request decrlpty key form authority and view response, request secret key and view response, download the file user.

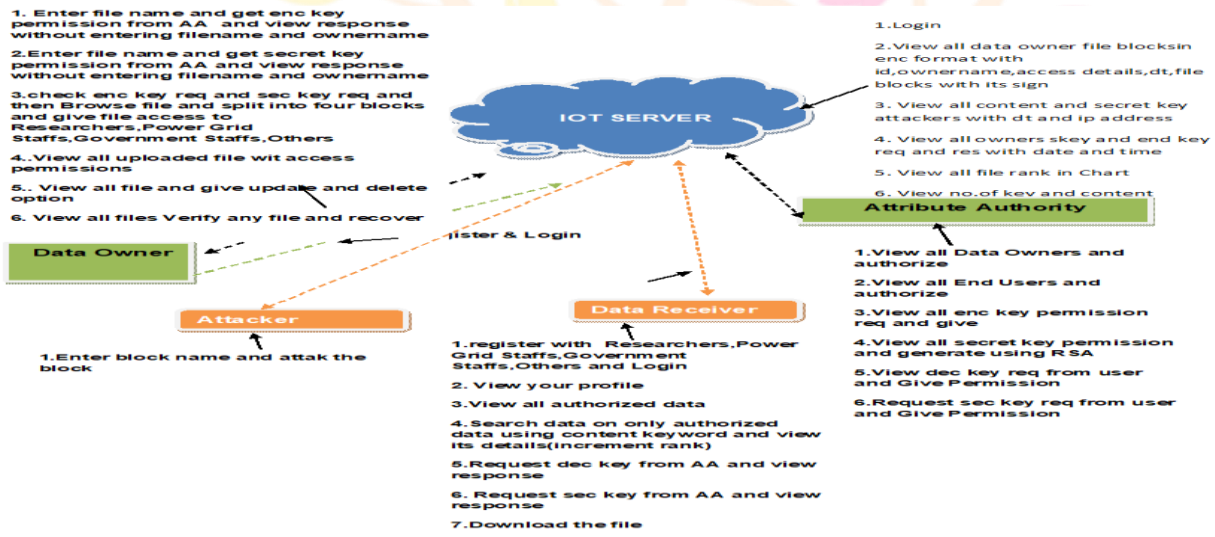


Fig.1 suggested system architecture

IV. RESULTS AND DISCUSSION

The output screens obtained after running and executing the system are shown from Fig.2 to Fig.8

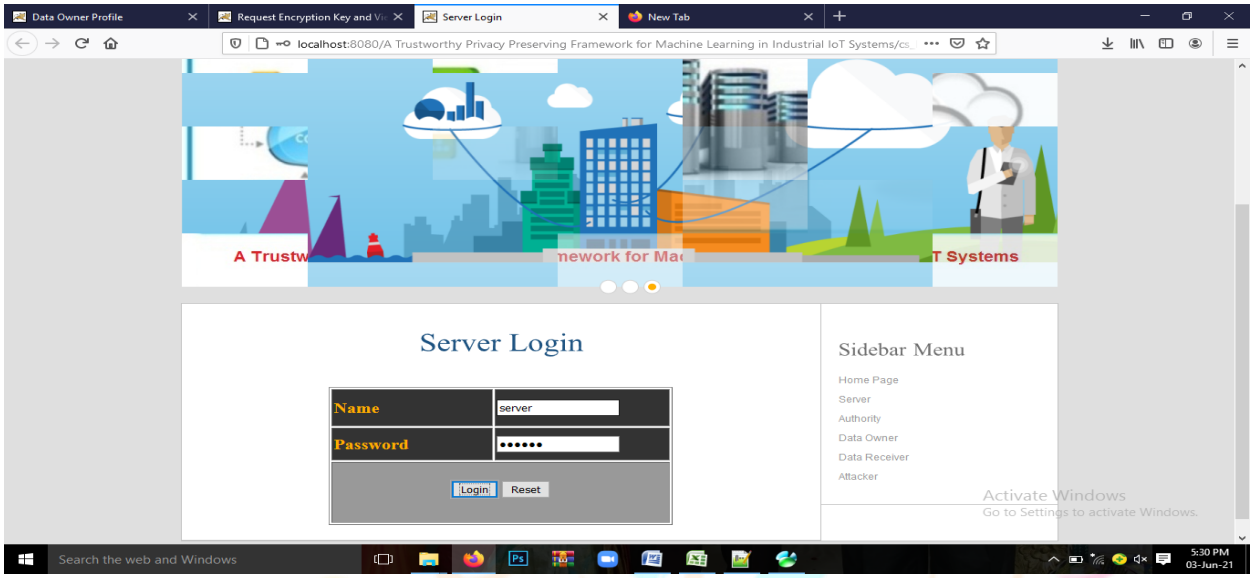


Fig.2 server login

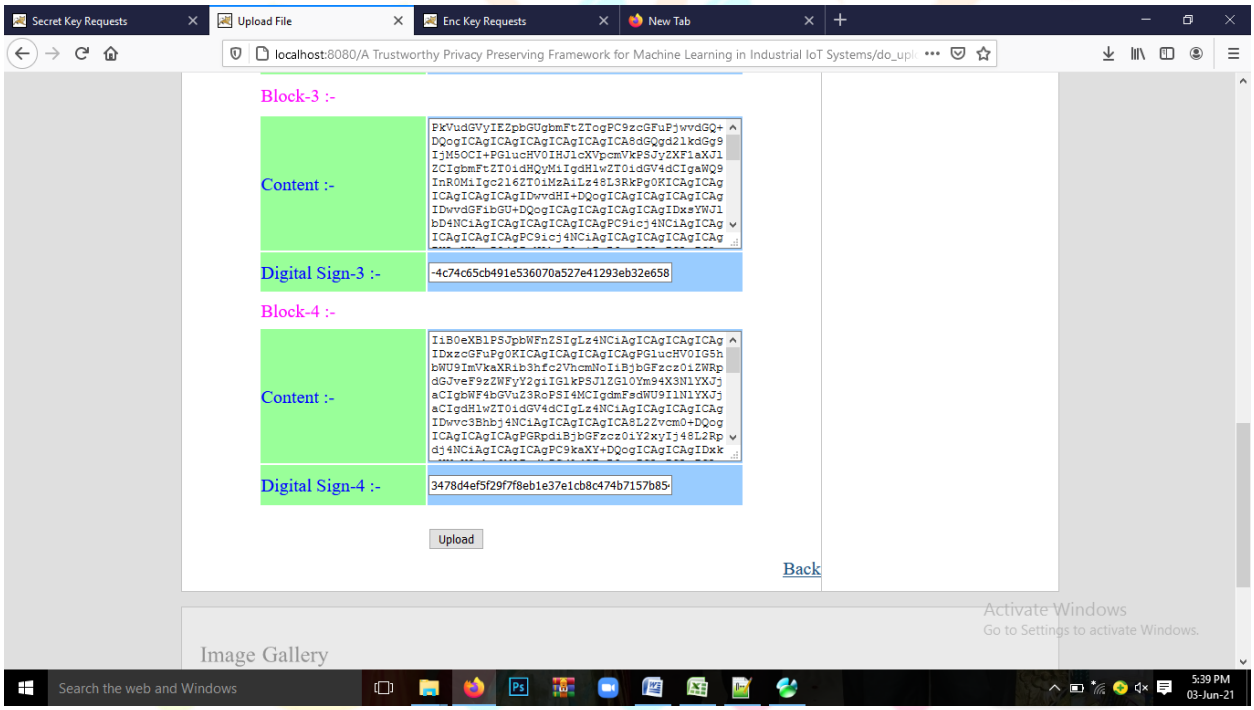


Fig.3 **Uploaded file in blocks**

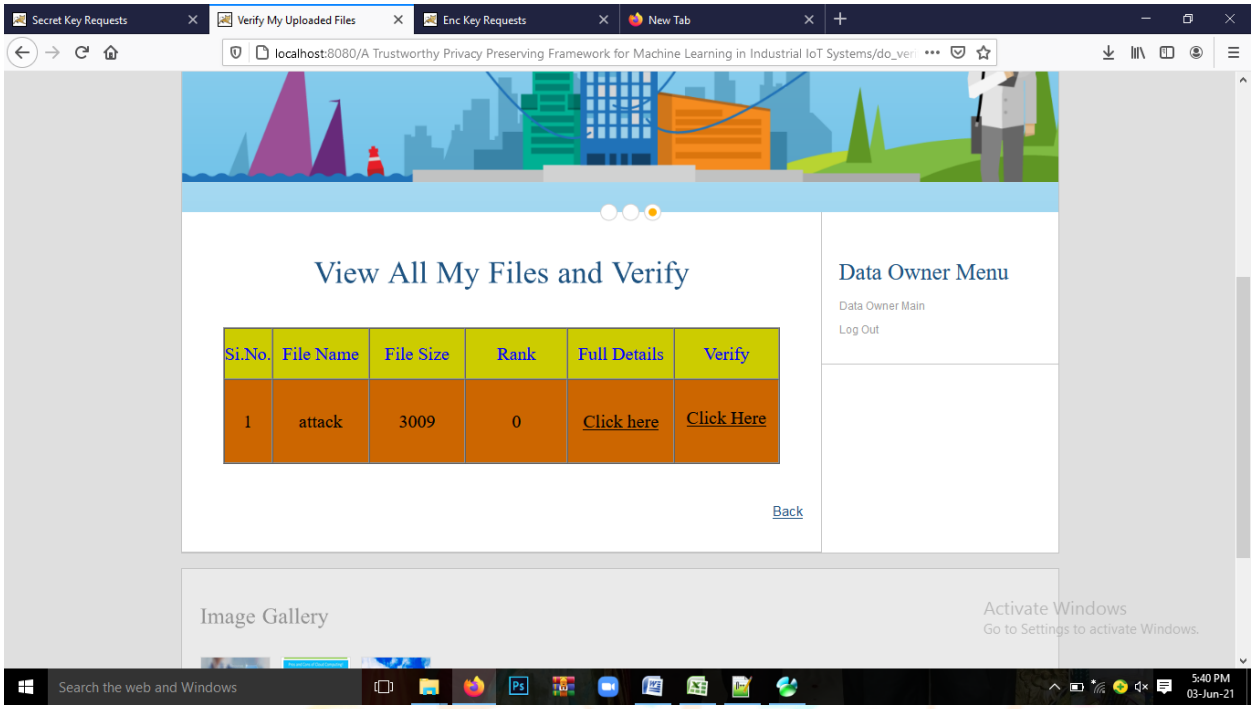


Fig.4 **view all files and verify**

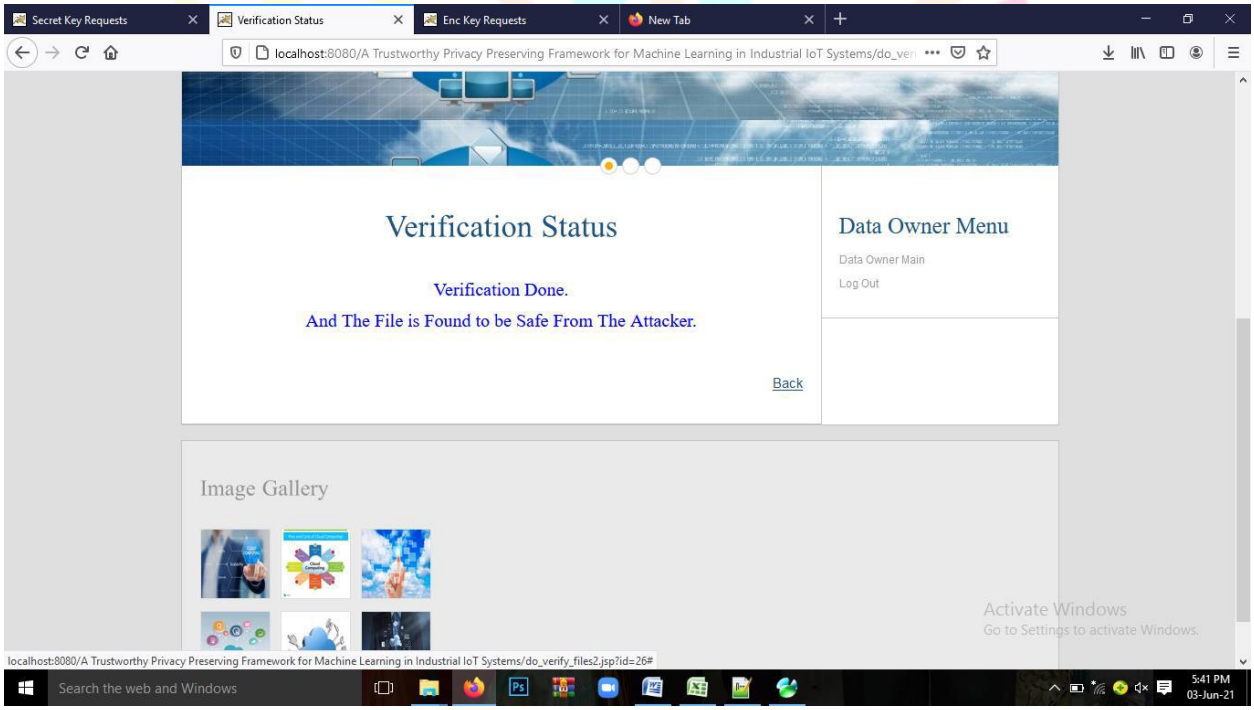
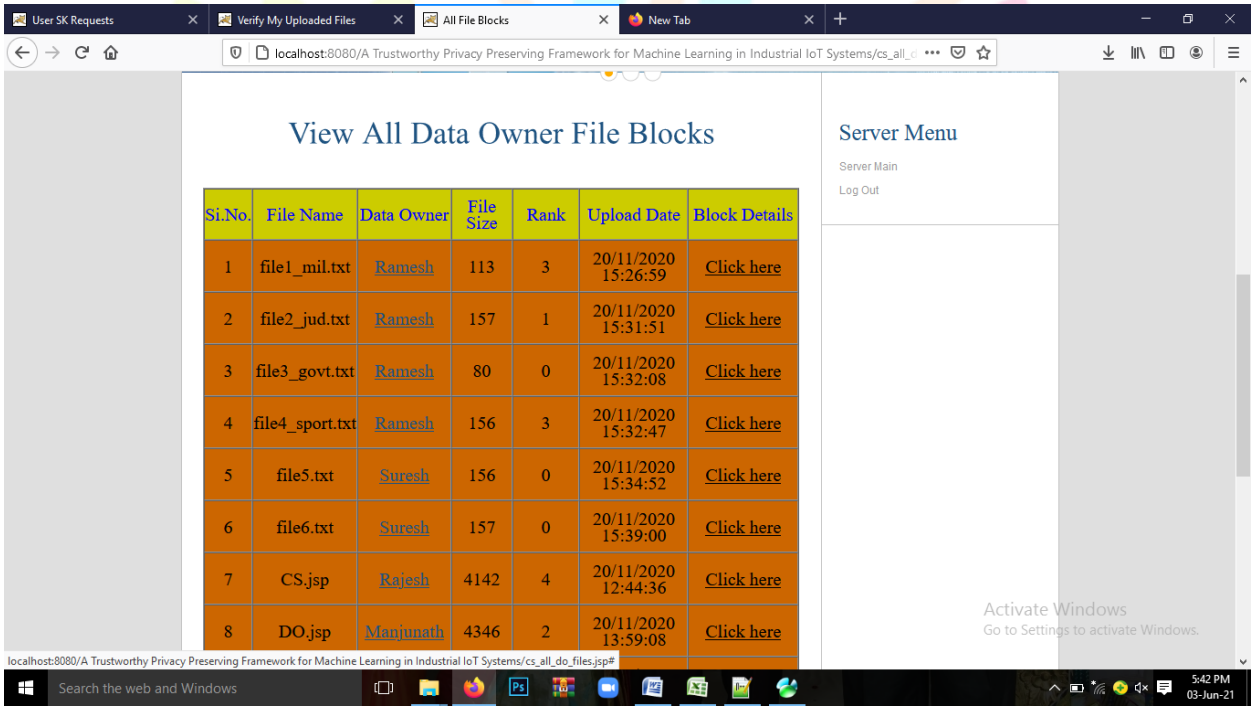


Fig.5 verification status

Fig.6 **View all file rank in chart**



Si.No.	File Name	Data Owner	File Size	Rank	Upload Date	Block Details
1	file1_mil.txt	Ramesh	113	3	20/11/2020 15:26:59	Click here
2	file2_jud.txt	Ramesh	157	1	20/11/2020 15:31:51	Click here
3	file3_govt.txt	Ramesh	80	0	20/11/2020 15:32:08	Click here
4	file4_sport.txt	Ramesh	156	3	20/11/2020 15:32:47	Click here
5	file5.txt	Suresh	156	0	20/11/2020 15:34:52	Click here
6	file6.txt	Suresh	157	0	20/11/2020 15:39:00	Click here
7	CS.jsp	Rajesh	4142	4	20/11/2020 12:44:36	Click here
8	DO.jsp	Manjunath	4346	2	20/11/2020 13:59:08	Click here

Fig.7 **View all data owner file blocks**

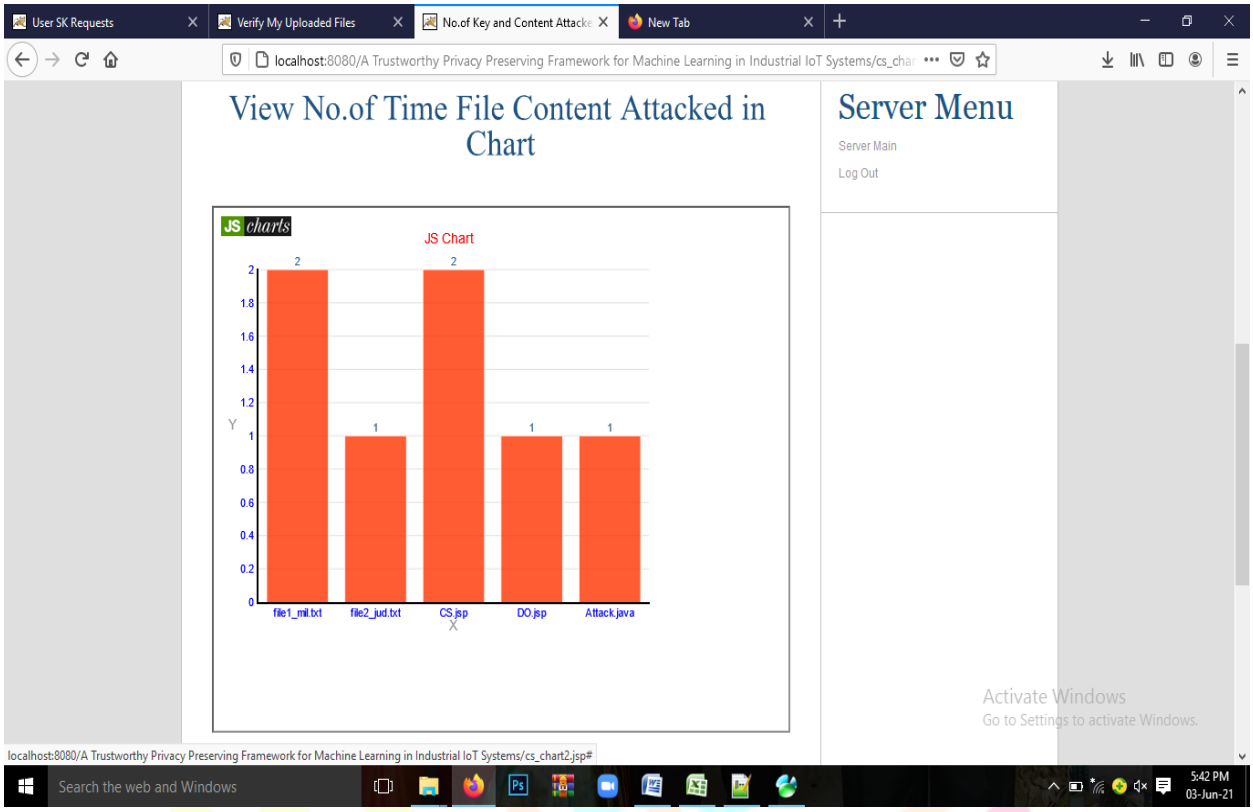


Fig.8**View time file content attacked in chart**

V. FUTURE SCOPE AND CONCLUSION

In this Project, proposed a new decentralized trust management protocol for IoT in computing architecture using a new consensus method. Each IoT object can assess trustworthiness of service providers and share it with IoT devices in a scalable way. Based on Blockchain technology, our protocol offers a global view on the trustworthiness of each data owner in the architecture. In Future work, we plan to extend our proposed countermeasure approach by developing more efficient offline algorithms for malicious nodes detection using machine learning techniques. Moreover, we consider the service composition effect on the trust assessment process.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourthquarter 2015.

[2] H. Al-Hamadi, R. Chen, and J.-H. Cho. Trust management of smart service communities. IEEE Access, 7:26362–26378, 2019.

[3] F. Bao, R. Chen, M. Chang, and J.-H. Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. On network and service management, 9(2):169–183, 2012.

[4] E. Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains. PhD thesis, 2016.

[5] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang. Trm-iot: A trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inf. Syst., 8(4):1207–1228, 2011.

[6] I. R. Chen, F. Bao, M. Chang, and J. H. Cho. Trust management for encounter-based routing in delay tolerant networks. In IEEE Global Telecommunications Conf. GLOBECOM, pages 1–6, Dec 2010.