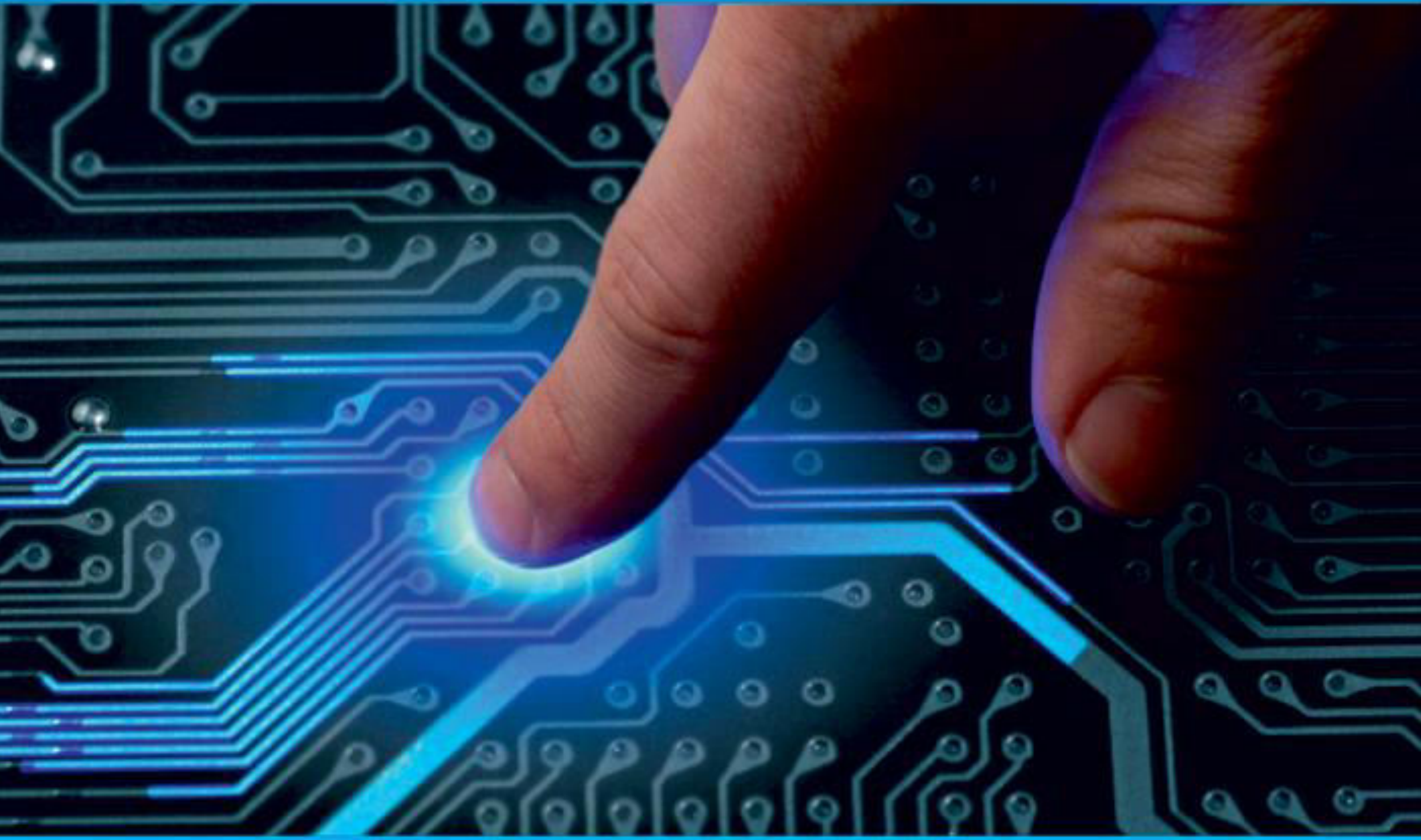
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009025 |

Blockchain-Enabled Fog Resource Access and Granting

Dhanushree N, Dr. M Siddappa

PG Student, Dept. of CSE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Professor and HOD, Dept. of CSE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, Karnataka, India

ABSTRACT: Haze registering is another figuring worldview for meeting inescapable immense access and lethargy fundamental applications by moving the dealing with limit closer to end clients. Haze registering is another figuring worldview for meeting inescapable immense access and lethargy fundamental applications by moving the dealing with limit closer to end clients. The topographical apportionment/floating features with potential freedom requirements familiarize new troubles with the regular methodology of association access control. In this paper, a blockchain-engaged fog resource access and giving plan is proposed to deal with the phenomenal necessities brought by dimness figuring. To meet huge access of fundamental applications by dealing with limit close to clients. The environment features with more potential requires known new troubles with regular method and the process of association access control. In this proposed paper, a block chain is used for accessing fog resources and provides a plan to deal with the proposed system. For every exchange discussion component upholds the haze asset supplier to powerfully distribute a proposition and works with the choice of the inclined toward resource close to the end client. Decentralized confirmation and endorsement facilitate the taking care of strain brought by tremendous access and single-point failure.

KEYWORDS: Haze registering, Single-point failure, BlockChain, Distributed Computing.

I. INTRODUCTION

Haze registering, based on the figure given below, explains how data expansion is done on the cloud platform and it is stored, which mainly handle limit, control, correspondence. Near with edge figuring idea, haze processing can ease the restrictions in current organization foundation and better help strategic, information thick use cases. Mist registering is much of the time wrongly called edge processing, however there are key contrasts.As its name recommends, haze is geologically circulated with vulnerability and insecurity, like the genuine mist that floats whereverwithout aproper shape. In haze cases, the geo-dispersed mist assets are unified as a universal asset pool.

II. TECHNICAL CHALLENGE

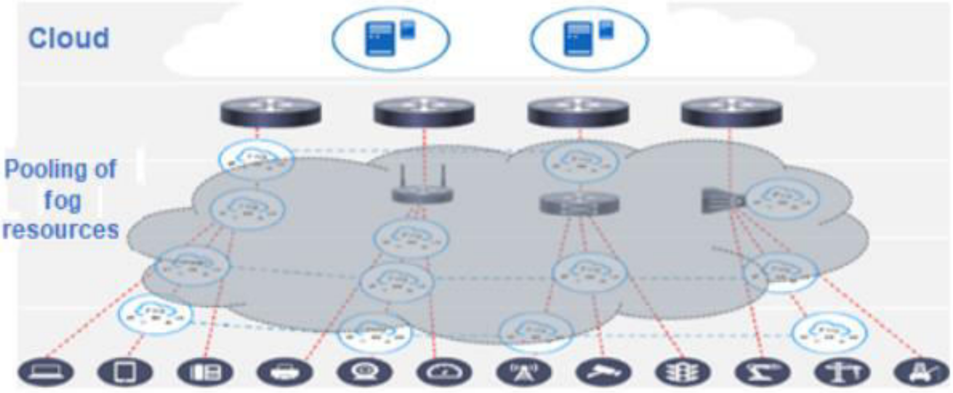


Fig 1: Fog Computing

Conversely, with conventional distributed computing, a few remarkable elements get very various issues mist registering situations. To start with, each haze hub should confirm the requestor and check getting to the mist resources right. In customary distributed computing, regularly an entrance is liable for all validation and approval activities. This concentrated admittance entrance plays out a brought together verification and approval method, and that implies that every supporter generally utilizes a static secret key/key to get to comparing assets until they mean or are expected to change the secret key/key. In like manner, the expense of a resource by and large is static and bound together paying little mind to the person is authorised to sign the authority to the third party to the resource unit who requests. All of the resources have a spot with the manager and a uniform access offer is given.

Then again, haze hub suppliers might conclude their own cost for an asset as per the expense, time, hub status and surprisingly, individual inclination. The endorsers have more options on haze hubs/suppliers, and accordingly may pick more practical hubs to satisfy their necessities. During the whole haze asset access and allowing system, a few issues arise.

A. Haze hub character and destination determination.

How should an ally the vendor will help to perform the target a quality of muddy of the points, but considering all the points which are split. In the course of accepting, generally use same kind and it can be focused for an endorser of apply a cloud resource.

B. Dynamic accreditation for every exchange.

In haze figuring, one supporter might submit asset solicitations to various haze hubs. This implies the endorser ought to submit different accreditation keys while mentioning different haze hubs.

II. LITERATURE SURVEY

In paper [1], the technology has reached the peak of hype. Yet, it could be on a vertical ascension once more. While the exciting ride of digital forms of money, for example, bitcoin has additionally projected slanders on blockchain innovation and it has — late occasions, for example, COVID-19 and its effect on the associated economy have made new objectives for digitizing exchanges.

How Blockchain Technology works?

To prevent data leakage and misusing, the culprit can attack the server where videos are stored in distributed aspect of blockchain will store the data and duplicate among different computers. The overt repetitiveness away brought by blockchain innovation brings additional security and improves information access since clients in IoT environments can submit to and recover their information from various gadgets.

Going on with this model, say the robber is caught and guarantees in court that the recorded video is fashioned proof. The permanence idea of blockchain innovation implies that any change to the put away information can be handily identified. In this manner, the robber's case can be checked by taking a gander at endeavors to mess with the information, he said. However, the decentralization part of blockchain innovation can be a significant issue while putting away information from IoT gadgets.

In paper [2], IoT makes our daily activities very easy and made us to live with the devices every day. This discovering the new devices and sensors brings the communication bring big concerns, and by using IoT communication brings concern mainly about data privacy and confidentiality.

In paper [3], Data security is a major issue and the challenge in IoT, but fortunately protocols used in this are slow and difficult to use. A new framework is used in the proposed system i.e., based on blockchain technology. Here, the contribution is to check the objectives of the proposed framework that enables uses to control and own the data. To enhance the model of implementation, need to use blockchain into access control manager.

Paper [4], In IoT, a flexible and trustworthy access control framework is of significance to ensure the security of lightweight IoT devices. The conventional centralized access control framework is no longer fit for the open and large-scale IoT environments. In this paper, proposed an attribute-based distributed access control framework (ADAC) for IoT using blockchain technology. SC and OC are responsible for managing subject attribute and object attribute information, respectively. PCs are used to manage access control policies. ACC performs authorization judgment by accessing attributes and policies. Finally, a case study is performed to demonstrate the workflow and show that ADAC could achieve fine-grained and flexible access control for IoT.

III. EXISTING SYSTEM

In the old access time, which is usually have authentication to enter the responsible authenticator by the actions.This will help to perform authentication and authorization procedure, which means user who are new will have unchangedkey to have access to the resources till have intend to change access the password.

IV. PROBLEM STATEMENT

Haze assets are genuinely situated on the organization edge, which is past the customary access entryway, e.g., broadband organization door and versatile administration element substances. By using access gateway, the traffic must travel through the round trip, this is due to last node cannot perform the access control.

V. OBJECTIVES

✓ Fog node identity and target node selection.
✓ Dynamic credential for each transaction.
✓ Dynamic independent offer provision.
✓ Authentication and resource offering.

- Mist hub character and target hub choice:

How could a supporter or application client be assisted at performing verification with target mist hubs, considering that these haze hubs are topographically conveyed? In distributed computing, for the most part utilize one uniform and unified verification entrance for a supporter of apply a cloud asset. In real time, while uploading data, selection of nodes occurs dynamically. But for ease of implement, selecting manually.

- Dynamic certification for every exchange:

In haze registering, one supporter might submit asset solicitations to various haze hubs. This implies the endorser ought to submit different qualification keys while mentioning different haze hubs. While in a distributed computing situation, an endorser typically just keeps one qualification for a cloud asset demand. Each time, while uploading the data into a server, dynamic credential should be generated for each transaction of block files.

- Dynamic free deal arrangement:

In haze figuring, different mist hubs might give different asset offers to requesters. Main server and Fog server should not be dependent on each other. As Metadata is stored in Fog server and Block data is in main server. While accessing the data, first communicate with fog server. By obtaining the metadata, then reach to main server.

- Validation and asset offering:

In regular haze situations, the asset access and conceding might be performed with per-exchange granularity. Any data to upload, download or to access, first have to authenticate by providing valid details. Once the authentication is valid, accessing the resources is possible.

VI. DESIGN OF A SYSTEM BLOCKCHAIN-ENABLED FOG RESOURCE ACCESS

The Smart understanding is the basic thought of the blockchain 2.0 structure. A splendid understanding is an executable code that unexpected spikes popular for the blockchain to work with, execute, and maintain the states of a comprehension between untrusted parties. It will in general be seen as a structure that releases electronic assets for all or a part of the intricate social events once the predefined rules have been met. Diverged from standard arrangements, wise arrangements don't rely upon a trusted in outcast to work, achieving low trade costs.

The brilliant agreement is the critical idea of the blockchain 2.0 framework. A brilliant agreement is an executable code that sudden spikes in demand for the blockchain to work with, execute and uphold the details of an understanding between untrusted parties. It tends to be viewed as a framework that discharges computerized resources for all or a portion of the elaborate gatherings once the predefined rules have been met. Contrasted with customary agreements, brilliant agreements don't depend on a confided in outsider to work, bringing about low exchange costs. Tending to the extraordinary difficulties and prerequisites introduced over, a brilliant agreement-based haze asset to take and give the policies which has been proposed and to enable the data to be centralised and resource are offering for each fog centre as shown in below figure.

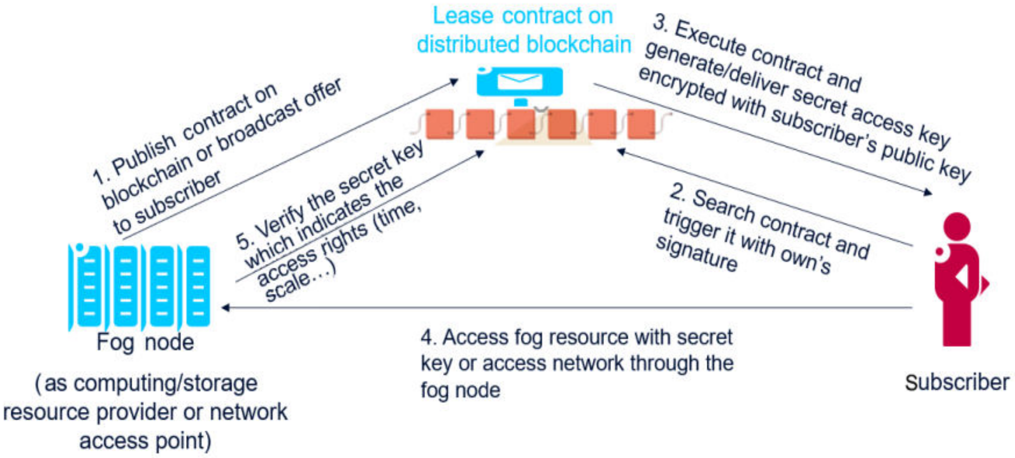

Lease contract on distributed blockchain
1. Publish contract on blockchain or broadcast offer to subscriber
3. Execute contract and generate/deliver secret access key encrypted with subscriber's public key
5. Verify the secret key which indicates the access rights (time, scale…)
2. Search contract and trigger it with own's signature
Fog node
(as computing/storage resource provider or network access point)
4. Access fog resource with secret key or access network through the fog node
Subscriber

Fig 2: Working flow of Fog resources

A. Shrewd agreement plan and execution.

The shrewd agreement idea is acquainted with empower dynamic, programmed certification age and conveyance for autonomous mist asset access and allowing. In this plan, a savvy contract is a progression of programming codes expected to carefully work with, check or uphold the exchange or execution of an agreement on haze asset access and conceding. A private blockchain was developed with a few Go-Ethereum clients [19], which act as excavator hubs and change the gadgets into an Ethereum node [20].Right when a fog centre will share its resources, it can introduce a complimentary housing contract.This kind of contract which is a part of the code to be executed and it tells how to know it has to be performed. In figure 4, it is very essential to store lease contract which are given for example. Then, the secret key is mixed with the visitor's public key to enable secure transport, as shown in Step 3 of fig. 2. The rent contract is posted on the blockchain with the mark of the asset supplier (haze hub for this situation). Each progression of the agreement execution should be affirmed with the agent's mark, which can ensure the non-disavowal. Similarly, as with the exemplary blockchain idea, all the agreement records are added and put away in the straight connected block. What's more, the whole blockchain is kept up with by thousands/a huge number of diggers, and any excavator can confirm every exchange or agreement execution utilizing the relating counterparty's public key. Hence, every one of the exchanges and agreements are discernible and irreversible.

Every asset supplier can have its own agreement, which might be unique in relation to those of other haze hubs. Not by any stretch like ordinary cloud procedure, each fog centre can independently give its own resource offer on the blockchain. During the execution of the impressive comprehension, a shrewd mystery key for the endorser is in this manner made, and it ought to be unscrambled by the partner.Contrasted and the conventional cloud arrangement in which generally only one key is given to an endorser, a smart contract-based arrangement upholds every supporter of purpose different mystery keys while getting to various haze hubs. The insightful agreement is stayed aware of on the blockchain by all the digger centres.

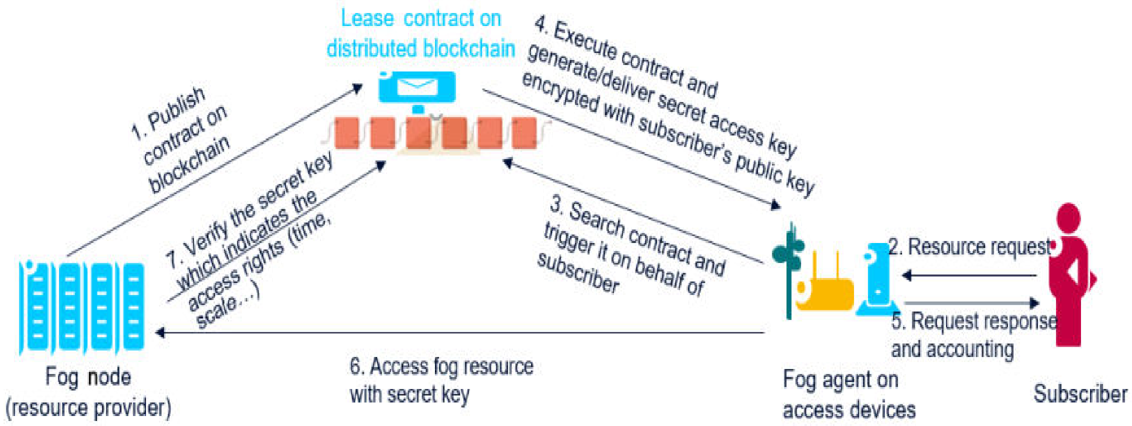

Lease contract on distributed blockchain
1. Publish contract on blockchain
4. Execute contract and generate/deliver secret access key encrypted with subscriber's public key
7. Verify the secret key which indicates the access rights (time, scale...)
3. Search contract and trigger it on behalf of subscriber
2. Resource request
5. Request response and accounting
6. Access fog resource with secret key
Fog node (resource provider)
Fog agent on access devices
Subscriber

Fig 3: Agent for the fog to access the driver.

B. Framework Implementation

Blockchain-empowered mist asset access. The ascent of blockchain innovation gives the likelihood to tackle the asset the executives issue of haze processing. Simultaneously, it cryptographically ensures the information's irreversible and unforgeable qualities and furthermore safeguards the information security of clients in the haze figuring climate.
Therefore, the primary goal of this project is to propose a fog computing resource contribution model based on an alliance chain and advances the blockchain system into the fog computing network architecture.

The fundamental responsibilities of this endeavor can be summarized as follows:

- A Blockchain-based fog enrolling resource responsibility model is proposed, which ponders a satisfaction degree (task culmination degree) as an evaluation record for organization given by dimness handling expert associations.
- Using differential game speculation to handle the proposed model, the numerical re-enactment is used to discuss the relationship between the best resource responsibility methodology of the cloudiness centre and the best benefit under the best framework.

V. FLOW CHART

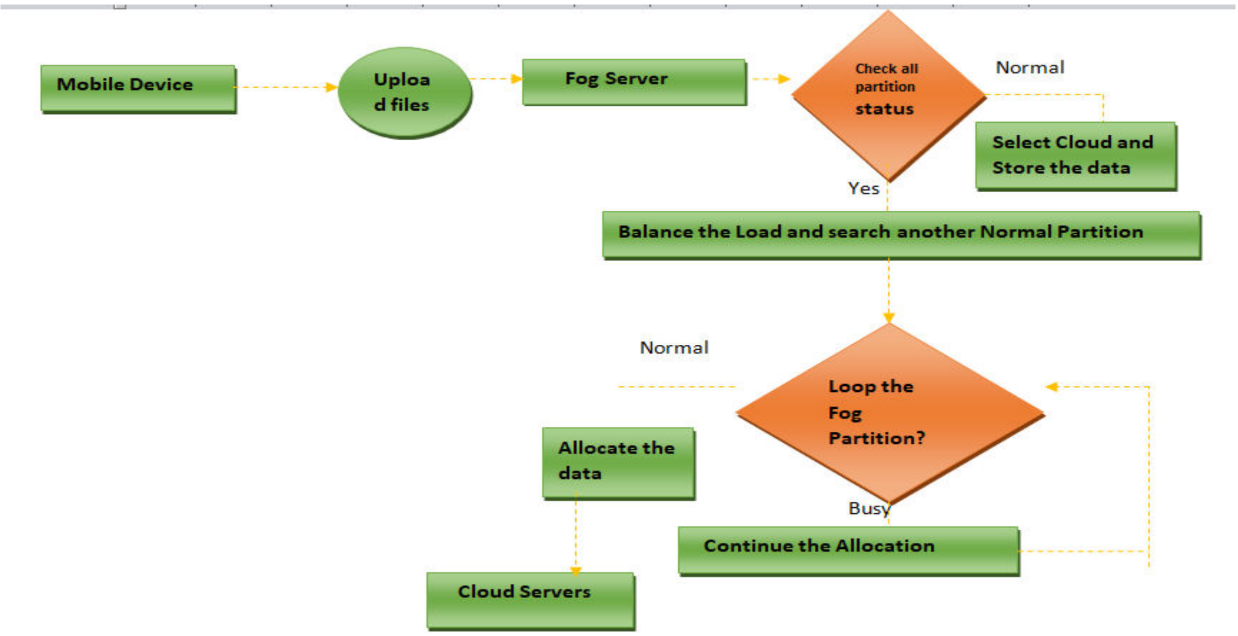


Fig 4: Flow chart of the system

The above flow chart shows that mobile users upload any file the request will go to fog server. It will check the partitions and status of each node and then select particular node to allocate resource to store that file basically, will balance load energy of each node.

VII. MODULES FOR IMPLEMENTATION

A. Cell phone

In this module, the cell phone goes about as information supplier which transfers their scrambled information in the Cloud server through haze server. For the security reason the information proprietor encodes the information document and afterward store in the server. The Data proprietor can have fit for controlling the Check all parcel status, Select the segment in light of the status (Idle or Normal), View all Partition status subtleties, Select the parcel and apportion the assets to comparing cloud, View all Transaction Details, View all cloud clients.

B. Cloud Server

The Cloud server oversees which is to give information capacity administration to the Data Owners. Information proprietors encode their information documents and store them in the Server for imparting to information customers and play out the accompanying activities like View all client records, View all cloud assailants and View all segments subtleties.

C. Mist Server

In this module, the Fog Server will play out the accompanying activities, for example, Check all parcel status, Select the segment in light of the status (Idle or Normal), View all Partition status details, Select the parcel and distribute the assets to comparing cloud, View all Transaction Details, View all cloud clients.

D. End User

In this module, the End User plays out the accompanying activity, for example, Register and Login, Request File Details/Receive the File Details, Request Secret Key.

VIII. APPLICATIONS

1. SMARTGRID: Smart grid is the next generation electric power distribution network. Smart grid gives an obvious energydistributionwhereserviceprovidersandcustomercanmonitorand control their pricing, production and consumption in realtime.
2. HEALTHCARESYSTEM: Fog computing plays an important role in emergencymedical service with little latency restrictions associated withimplantable medical devices, ambulance communications orportable access to patient medical files.
3. TRAFFICCONTROLSYSTEM: In traffic control system, the video camera that detects the flashing lights of an ambulance can automatically change the streetlightsandopenthetracksforthevehicletocrossthetraffic.

IX. RESULTS

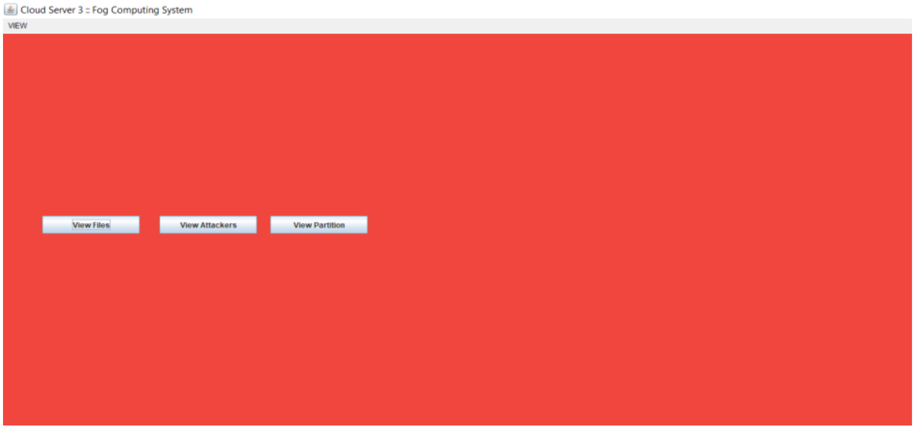


Fig 5: Login Page

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009025 |

The above figure shows the login page of a cloud server to provide the communication.

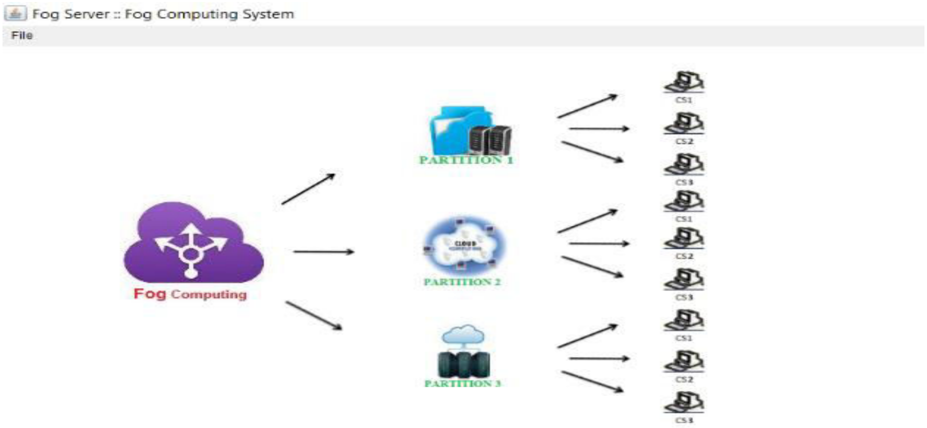
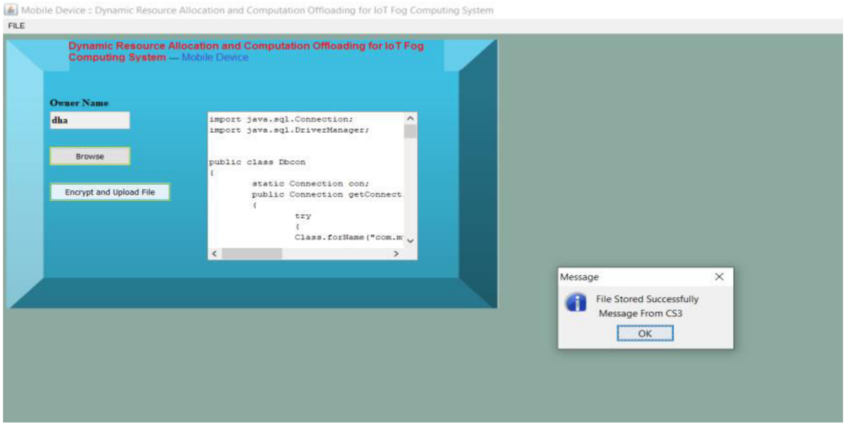


Fig 6: Dynamic allocation Resources page

This page indicates that the file is uploading from Fog server to Cloud server.


Mobile Device :: Dynamic Resource Allocation and Computation Offloading for IoT Fog Computing System
FILE
Dynamic Resource Allocation and Computation Offloading for IoT Fog Computing System --- Mobile Device
Browse
Encrypt and Upload File
Message
OK

Owner Name: dha

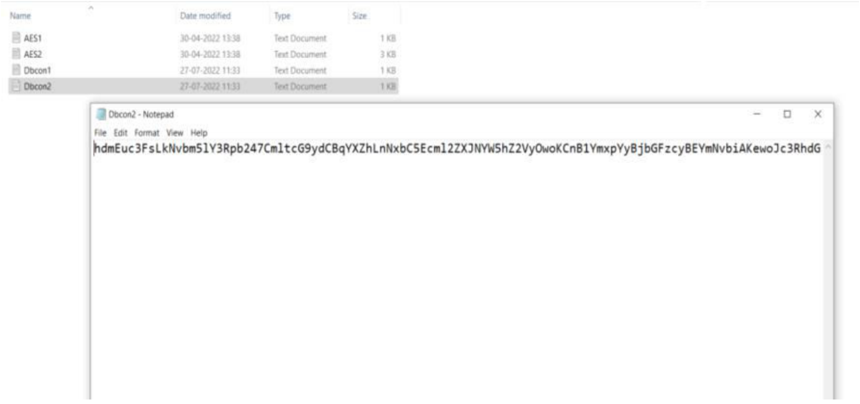
```
import java.sql.Connection;
import java.sql.DriverManager;


public class Dbcon
{
        static Connection con;
        public Connection getConnect
        {
                try
                {
                Class.forName("com.m
```

File Stored Successfully
Message From CS3

Fig 7: File stored into the selected cloud server.

The above figure shows File is stored successfully in the cloud server.

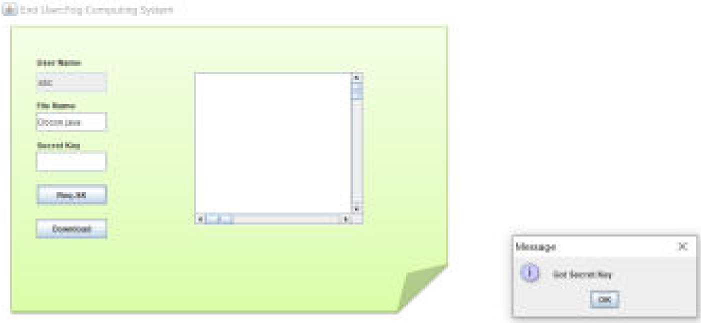


Name	Date modified	Type	Size
AES1	30-04-2022 13:38	Text Document	1 KB
AES2	30-04-2022 13:38	Text Document	3 KB
Dbcon1	27-07-2022 11:33	Text Document	1 KB
Dbcon2	27-07-2022 11:33	Text Document	1 KB

```
hdmEuc3FsLkNvbm51Y3Rpb247CmltcG9ydCBqYXZhLnNxbC5Ecml2ZXJNYW5hZ2VyOwoKCnB1YmxpYyBjbGFzcyBEYmNvbiAKewoJc3RhdG
```

Fig 8: Shows data encrypted and stored.

The above figure shows data is encrypted and stored in the form of block files.



End User::Fog Computing System

User Name

abc

File Name

Dbcon.java

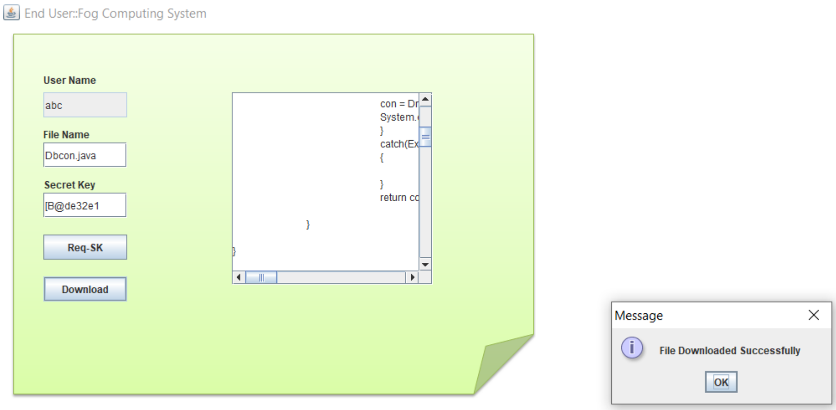
Secret Key

Message

Got Secret Key

Fig 9: Shows secret key generated

The above figure shows the generation of the secret key, to obtain the file.



End User::Fog Computing System

User Name

abc

File Name

Dbcon.java

Secret Key

[B@de32e1

```
con = Dr
System.
}
catch(Ex
{

}
return cc
   }
}
```

Message

File Downloaded Successfully

Fig 10: The data is downloaded successfully

The downloaded data shows in above figure is now the file in readable format.

X. CONCLUSION

Mist figuring assumes a vital part in fulfilling the prerequisites of deferral delicate applications, like VR, AR and modern creation lines. Haze hubs are likewise a kind of organization asset, yet they have novel qualities: geo-disseminated, independent and free contributions.

REFERENCES

1. T. M. Fernandez-Caram´es and P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access, vol. 6, pp. 32979–33001, 2018.
2. O. J. A Pinno, A. R. A. Gregio, and L. C. E. De Bona, ControlChain: Blockchain as a central enabler for access control authorizations in the IoT, in Proc. 2017 IEEE Global Communications Conf., Singapore, 2017, pp. 1–6.
3. A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, FairAccess: A new blockchain-based access control framework for the Internet of Things, Security and Communication Networks, vol. 9, pp. 5943–5964, 2016.

4. P. Wang, Y. L. Yue, W. Sun, and J. J. Liu, An attribute-based distributed access control for blockchain-enabled IoT, in Proc. 2019 Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 2019, pp. 1–6.
5. G. Guerrero-Contreras, J. L. Garrido, S. Balderas-Diaz, and C. Rodriguez-Dominguez, "A context-aware architecture supporting service availabilityin mobile cloud computing," IEEE Transactions on Services Computing,vol. 10, no. 6, pp. 956-968, Nov.-Dec. 2017.
6. X. Guo, L. Liu, Z. Chang, and T. Ristaniemi, "Data offloading and taskallocation for cloudlet-assisted ad hoc mobile clouds," Wireless Networkvol. 24, no. 1, pp. 79-88, Jan. 2018.
7. Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computingfor connected vehicles: A deep reinforcement learning approach,"IEEE Trans. Vehicular Technology, vol. 67, no. 1, pp. 44-55, Jan. 2018.
8. N. Zhao, X. Liu, F. R. Yu, M. Li, Victor C. M. Leung, "Communications,caching, and computing oriented small cell networks with interferencealignment," IEEE Communications Magazine, vol. 54, no. 9, pp. 29-35,Sept. 2016.
9. L. Liu, Z. Chang, X. Guo, S. Mao, and T. Ristaniemi, "Multi-objectiveoptimization for computation offloading in fog computing," IEEE Internetof Things Journal, vol. 5, no. 1, pp. 283-294, Feb. 2018.
10. A. Arins, “Blockchain based Inter-domain Latency Aware RoutingProposal in Software Defined Network,” inProceedings of IEEE 6thWorkshop on Advances in Information, Electronic and Electrical Engineering(AIEEE),Nov. 2018, pp. 1–2.
11. C. Lin, D. B. He, X. Y. Huang, K. K. R. Choo, and A. V. Vasilakos, BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2018.
12. P. K. Sharma, M. Chen, and J. H. Park, “A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT,” IEEE Access,vol. 6, pp. 115–124, Sep. 2018.
13. X. Jiang, M. Z. Liu, C. Yang, Y. H. Liu, and R. L. Wang, A blockchain-based authentication protocol for WLAN mesh security access, Computers, Materials and Continua, vol.58, no. 1, pp. 45–59, 2019.
14. Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, “Cochain-SC: An IntraandInter-Domain Ddos Mitigation Scheme Based on Blockchain UsingSDN and Smart Contract,” IEEE Access, vol. 7, pp. 98 893–98 907, Jul.2019.
15. M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard,“STewARD:SDN and Blockchain-Based Trust Evaluation for AutomatedRisk management on IoT Devices,” in Proceedings of IEEEConference on Computer Communications Workshops (INFOCOM WKSHPS),Apr. 2019, pp. 841–846.
16. L. Xie, Y. Ding, H. Yang, and X. Wang, “Blockchain-Based Secure andTrustworthy Internet of Things in SDN-Enabled 5G-VANETs,” IEEEAccess, vol. 7, pp. 56 656–56 666, Apr. 2019.
17. Y. Y. Zhang, S. Kasahara, Y. L. Shen, X. H. Jiang, and J. X. Wan, Smart contract-based access control for the Internet of Things, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2019.
18. Y. L. Chen, X. J. Wang, Y. L. Yang, and H. Li, Locationaware Wi-Fi authentication scheme using smart contract, Sensors, vol. 20, no. 4, p. 1062, 2020.
19. Geth client for building private blockchain networks, https://github.com/ethereum/go-ethereum, 2021.
20. V. Buterin, A next-generation smart contract and decentralized application platform, https://ethereum.org/en/whitepaper/, 2021.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com