ADVANCING CONFIDENTIALITY IN IOT HEALTH ASSISTANCES UTILIZING FOG COMPUTING

1Dr. T. CHARAN SINGH, 2S. SNEHA, 3Y. MOHAN VAMSHI, 4MRITYUNJAY KUMAR JHA

1Associate Professor, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad

234Under Graduate, Department of AI&DS, Sri Indu College of Engineering and Technology-Hyderabad

ABSTRACT

Internet of Things (IoT) is the interconnection of physical objects or devices that can transmit and receive data through the internet without human involvement. With the advancement in IoT devices particularly in healthcare sector, huge amount of data is collected from different sensors and all this data are transferred and stored in cloud. It becomes difficult to handle suchhuge amount of data in cloud specially the healthcare data where it requires real time data computation and storage. Security of the data is also major challenge in cloud. Fog computingis the answer to overcome the challenges. Fog nodes works at the edge side and enhances datasecurity, accuracy, consistency and reduces the latency rate which is an important factor for application like medical data. Implementation work is also described in the paper where a digital human temperature sensor device is built using DS18B20 temperature sensor. The datacollected from it is being encrypted in fog node using Advance Encryption Standard(AES) algorithm and it is send to cloud. Therefore, the security of the health care data is enhanced using Fog computing.

Keywords: IOT HEALTHCARE, FOG COMPUTING, CONFIDENTIALITY.

INTRODUCTION

Cloud computing provides a variety of IoT services, including computation resources, storage capacities, heterogeneity, and high processing that have accompanied a technological revolution. At many levels, the cloud allows for the virtualization of computational resources. Almost every aspect of human life has embraced cloud computing. Cloud computing, on the other hand, has limitations in termsof large delays, which have a negative impact on IoT jobs that demand a real-time reaction. It also doesnot work with industrial control systems that require a quick response time. A concept of fog computing has been introduced to link IoT devices with data centers. Similar to IoT, fog computing has several applications like monitoring and analysis of data from network- connected things in real time and facilitates further actions to be taken.

Fog computing is more virtualized and it can provide networking services among end devices and cloud computing data centers,but it is not entirely positioned at the edge of the network. Fog computing can be used at three levels of networking. The IoT is considered as a dynamic global network infrastructure, in which the things with unique characteristics are unified to enable advanced services. One of the basic technologies used in IoT healthcare is the Wireless Body Area Networks (WBANs). It can acquire the signals like body temperature, electrocardiogram (ECG), electromyography (EMG), and blood pressure. These data are transmitted to the end-users through the protocols like Wi-Fi or IEEE.802.15.4 for diagnosis and visualization.

In healthcare monitoring, the remote cloud servers are in use to process and store the data from sensor nodes using cloud computing. But there are some challenges like latency sensitivity, large data transmission, and location awareness. Fog computing brings cloud capabilities closer to end-users by delivering storage, processing, and communication to edge devices, which improve mobility, privacy, security, low latency, and network bandwidth. Fog computing can ideally match latency-sensitive or real-time applications. In today's rapidly evolving healthcare landscape, the integration of the Internet of Things (IoT) has played a pivotal role in transforming the way healthcare services are delivered. IoT devices have the potential to monitor patients, gather critical health data, and provide real-time assistance, enhancing patient care and reducing the burden on healthcare providers. However, with these advancements comesignificant challenges, particularly in ensuring the confidentiality and security of sensitive health information.

The burgeoning field of IoT health assistance and how Fog Computing can be leveraged to address the critical issue of confidentiality in healthcare IoT applications. Fog Computing, an extension of cloud computing, brings computation and data storage closer to the edge of the network,providing several advantages such as reduced latency, increased efficiency, and improved data privacy. By examining the synergy between IoT and Fog Computing, we aim to shed light on innovative solutionsfor safeguarding health data while reaping the benefits of connected healthcare.

LITERATURE SURVEY

TITLE: Enhancing Data Security in IoT Healthcare Services using Fog Computing.

AUTHORS: Saloni Alhat, Nikita Bangal, Aishwarya Gaikwad, Smita Khairnar. ABSTRACT: Security of the data is also major challenge in cloud. Fog computing is the answer to overcome thechallenges. Fog node works at the edge side and enhances data security, accuracy, consistency and reduces the latency rate which is an important factor for application like medical data. In this paper we will detect the heart disease by using sensors and pulse rate. The data detected will be stored in the fog node .The result would be display by the system as well as report will be sent through mail to the patient. The data collected from it is being encrypted in fog node using Advance Encryption Standard (AES) algorithm and it is send to cloud. Therefore, the security of the health care data is enhanced using Fog computing.

TITLE: Privacy and Security in Fog-Enabled IoT Applications: Challenges and Solutions.

AUTHORS: Mais Tawalbeh, and Muhannad Quwaider

ABSTRACT: The proliferation of Internet of Things (IoT) devices in various domains, particularly in healthcare, has necessitated the development of robust security and privacy frameworks to protect sensitive data. Fog computing, which extends cloud services to the edge of the network, presents a promising paradigm for addressing the latency and bandwidth limitations of traditional cloud computing. However, integrating fog computing with IoT introduces a unique set of challenges in ensuring data privacy and security. This paper provides a comprehensive review of the privacy and security issues in fog-enabled IoT applications, with a particular focus on healthcare systems. It identifies key challenges such as data encryption, secure data transmission, authentication, access control, and intrusion detection. The paper also reviews existing solutions and frameworks that have been proposed to mitigate these challenges, including advanced encryption techniques, blockchain integration, lightweight cryptographic protocols, and machine learning-based anomaly detection. Through this detailed analysis, the paper aims to highlight the importance of a multi- layered security approach that combines both technical and procedural measures.

TITLE: Enhancing Data Privacy in IoT-Driven Health Care Systems with Fog Computing.

AUTHOR: Alex J. Thompson, Emily R. Zhang.

ABSTRACT: The integration of Internet of Things (IoT) in healthcare systems has revolutionized the way medical data is collected, analyzed, and utilized, offering significant improvements in patient care and operational efficiency. However, this increased connectivity and data exchange have raised critical concerns regarding data privacy and security. Fog computing, an extension of cloud computing, emerges as a promising solution to address these issues by providing decentralized data processing closer to the data source. This paper explores the application of fog computing in IoT- driven healthcare systems to enhance data privacy. We propose a comprehensive framework that leverages fog computing to mitigate privacy risks through distributed data processing, localized storage, and secure data transmission protocols. The proposed framework is evaluated through a series of simulations and case studies, demonstrating its effectiveness in reducing latency, improving data security, and ensuring compliance with data privacy regulations. Our findings suggest that fog computing can significantly enhance the privacy and security of sensitive health data, making it a viable solution for modern healthcare systems.

SYSTEM ANALYSIS

EXISTING SYSTEM

Currently fog uses the Decoy system as a security service from malicious attacker. Like in Cloud, Fog uses this method to trick the attacker by providing fake data when they try to extract the data. In the decoy system the user has to sign up then login, while logging in the system will ask security questions related toinformation given while signing up. So when an attacker tries to login her/she will be trapped with the question and the system will give back spurious file which is very such similar to the original file and when the attackers tries to download it will turn out to be a fake data. But there is chance that the attacker might guess the questionsright. Therefore, this system is not a very good way of securing data.

DISADVANTAGES OF THE EXISTING SYSTEM

In the decoy system the user has to sign up then login, while logging in the system will asksecurity questions related to information given while signing up.

It become a bottle neck problem when it comes to real time data operation which is the majordrawback in the existing IoT healthcare system.

PROPOSED SYSTEM

In the proposed system a three tier architecture model. First layer will be the Edge devices which will collect the data and this data will be transferred to the middlelayer. The middle layer will be the fog layer; encryption process of the collected data will be performed in this layer. The encrypted data from the middle layer will then be send to the third layer which is the cloud layer. In the cloud the final encrypted data will be permanently stored.

The proposed system "Advancing Confidentiality in IoT Health Assistance Utilizing Fog Computing" appears to focus on enhancing the security and privacy of Internet of Things (IoT) devicesused in health assistance by leveraging fog computing technology.

ADVANTAGES OF PROPOSED SYSTEM

In order to overcome the problem Fog Computing concept has been introduced. Fog Computing inan archetype that extends the cloud computing platform. Fog acts as a middle layer between the cloud server and the end devices.

It enhances data security , accuracy, consistency and reduces the latency rate which is an importantfactor for application like medical data. As wellas the overall bandwidth to cloud is saved, thus achievingbetter quality of service.

IMPLEMENTATION AND RESULTS

1. User Module: The User module allows end-users to interact with the system for retrieving and downloading data. Users can search for specific files stored in the system and view or download them based on access permissions. This module primarily ensures secure and efficient data access for authorized users.

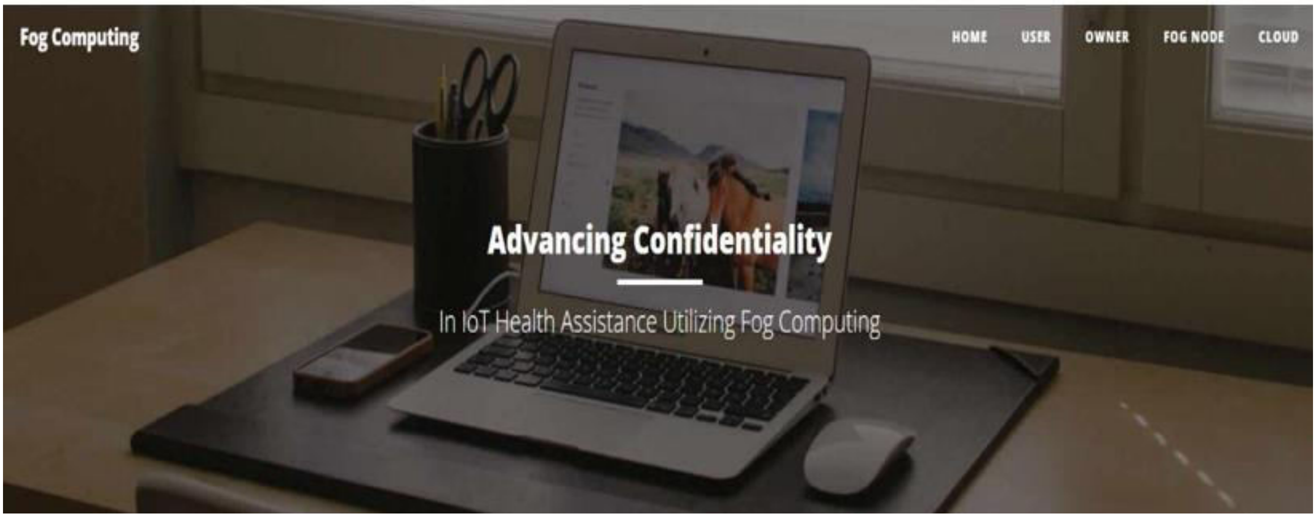
2. Owner Module: The Owner module is responsible for managing the data uploaded to the system. File owners can log in to their profile, upload new files to the cloud or fog node, and view a list of their uploaded files. This module provides full control over the data shared with the system and ensures accountability and traceability.

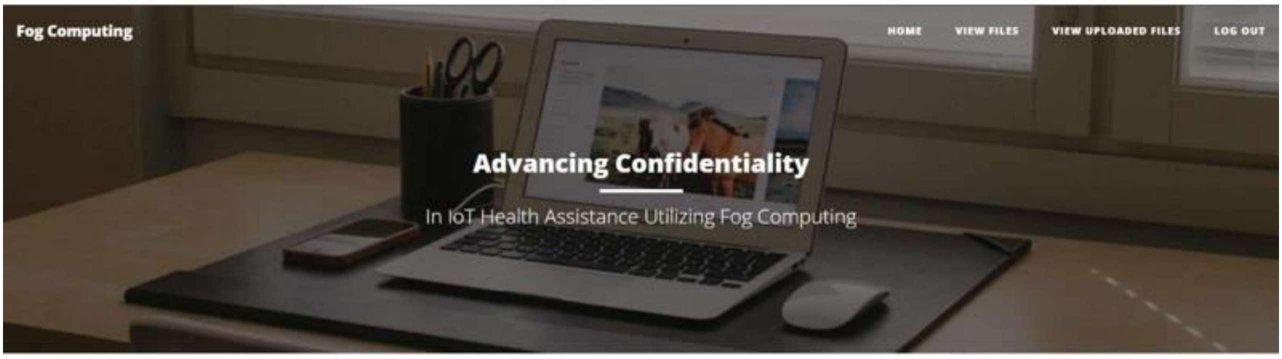
3. Fog Node Module: The Fog Node module acts as an intermediary layer between the user and the cloud, offering enhanced performance and reduced latency. It allows administrators or fog node operators to view all files processed or temporarily stored in the fog environment. This supports faster access and distributed computing.

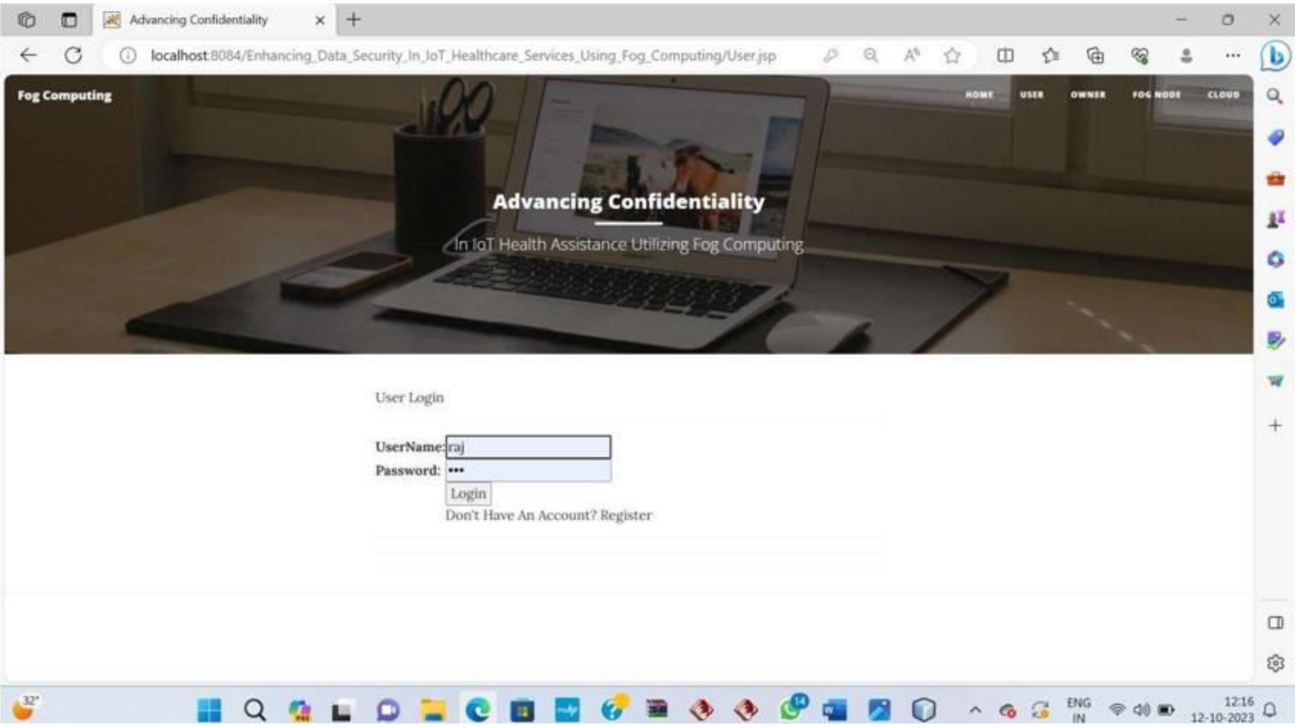
4. Cloud Module: The Cloud module handles long-term storage and data analytics. It allows cloud administrators to view all uploaded files across the system and analyze download activities. Additionally, it provides visual representations of file downloads through charts to assist in usage monitoring and reporting.

HOME PAGE

The term "Home screen" refers to the main or initial screen of an application or website that users encounter upon opening the application or accessing the website. The home screen is essentially the starting point and often sets the tone for the rest of the user experience.


Fog Computing
HOME
USER
OWNER
FOG NODE
CLOUD
Advancing Confidentiality
In IoT Health Assistance Utilizing Fog Computing

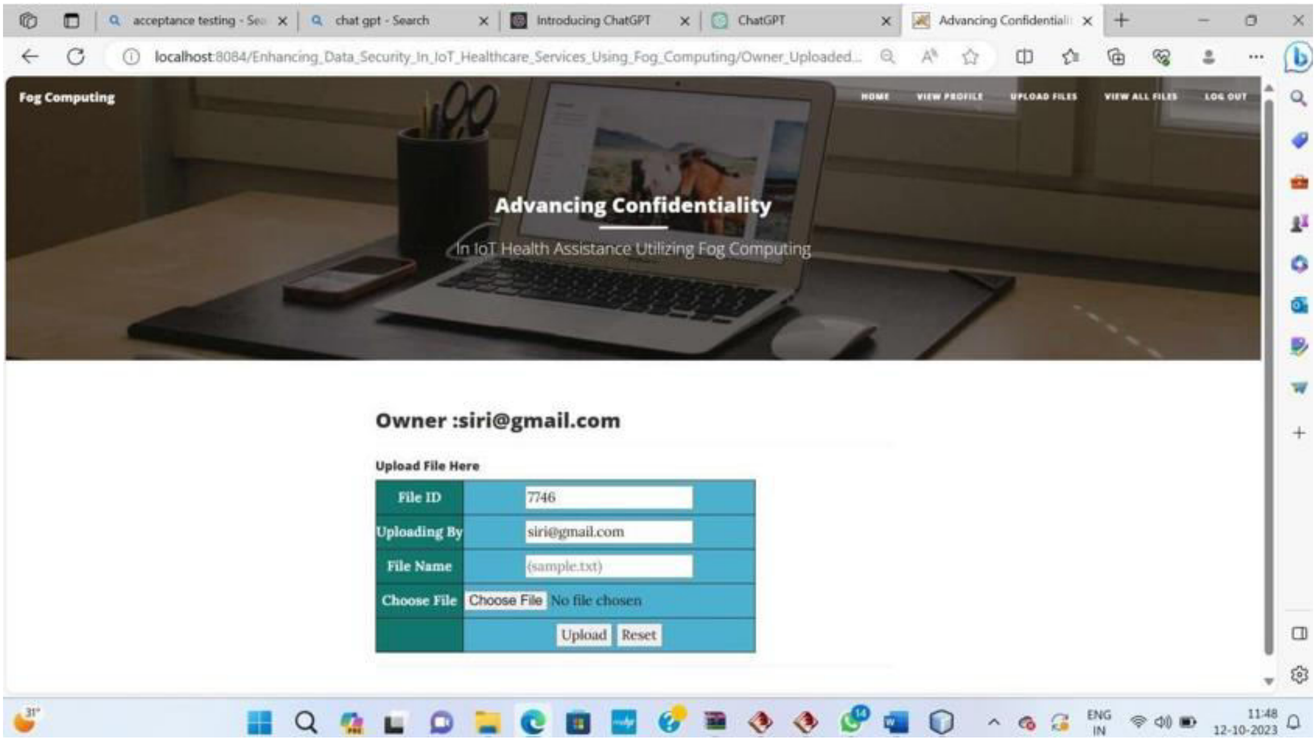

Fog Computing
HOME
VIEW FILES
VIEW UPLOADED FILES
LOG OUT
Advancing Confidentiality
In IoT Health Assistance Utilizing Fog Computing


Advancing Confidentiality
localhost:8084/Enhancing_Data_Security_In_IoT_Healthcare_Services_Using_Fog_Computing/User.jsp
Fog Computing
HOME
USER
OWNER
FOG NODE
CLOUD
Advancing Confidentiality
In IoT Health Assistance Utilizing Fog Computing
Login
12:16
12-10-2023

User Login

UserName: raj
Password: •••

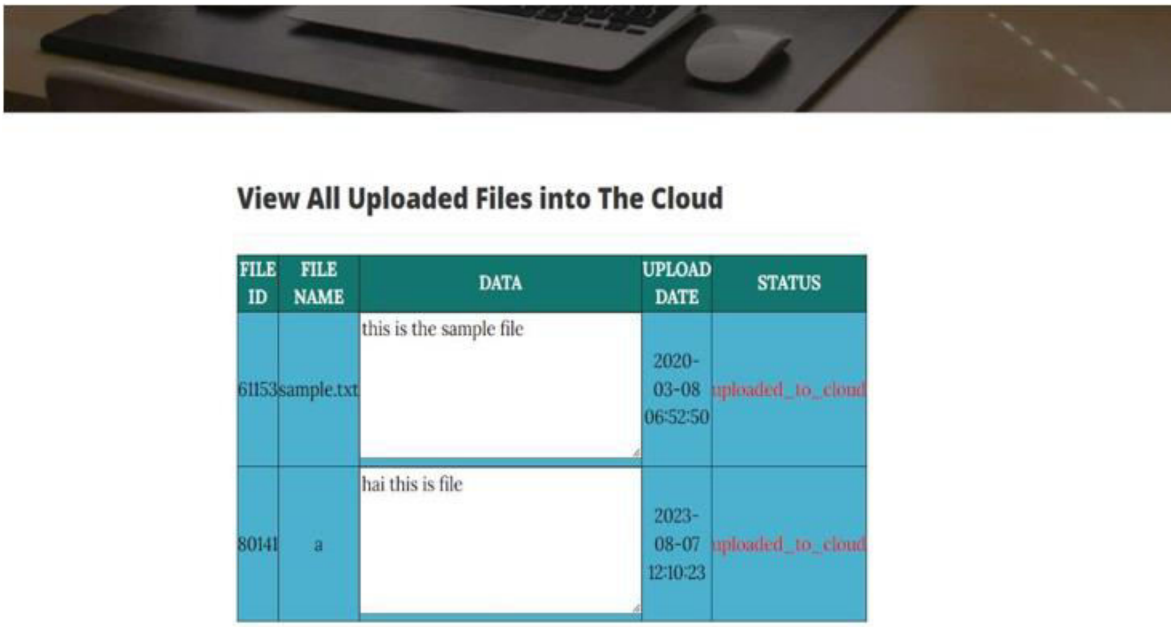
Don't Have An Account? Register


acceptance testing - Sea
chat gpt - Search
Introducing ChatGPT
ChatGPT
Advancing Confidentiali
localhost:8084/Enhancing_Data_Security_In_IoT_Healthcare_Services_Using_Fog_Computing/Owner_Uploaded...
Fog Computing
HOME
VIEW PROFILE
UPLOAD FILES
VIEW ALL FILES
LOG OUT
Advancing Confidentiality
In IoT Health Assistance Utilizing Fog Computing
ENG
IN
11:48
12-10-2023

Owner :siri@gmail.com

Upload File Here

File ID	7746
Uploading By	siri@gmail.com
File Name	(sample.txt)
Choose File	Choose File No file chosen
	Upload Reset

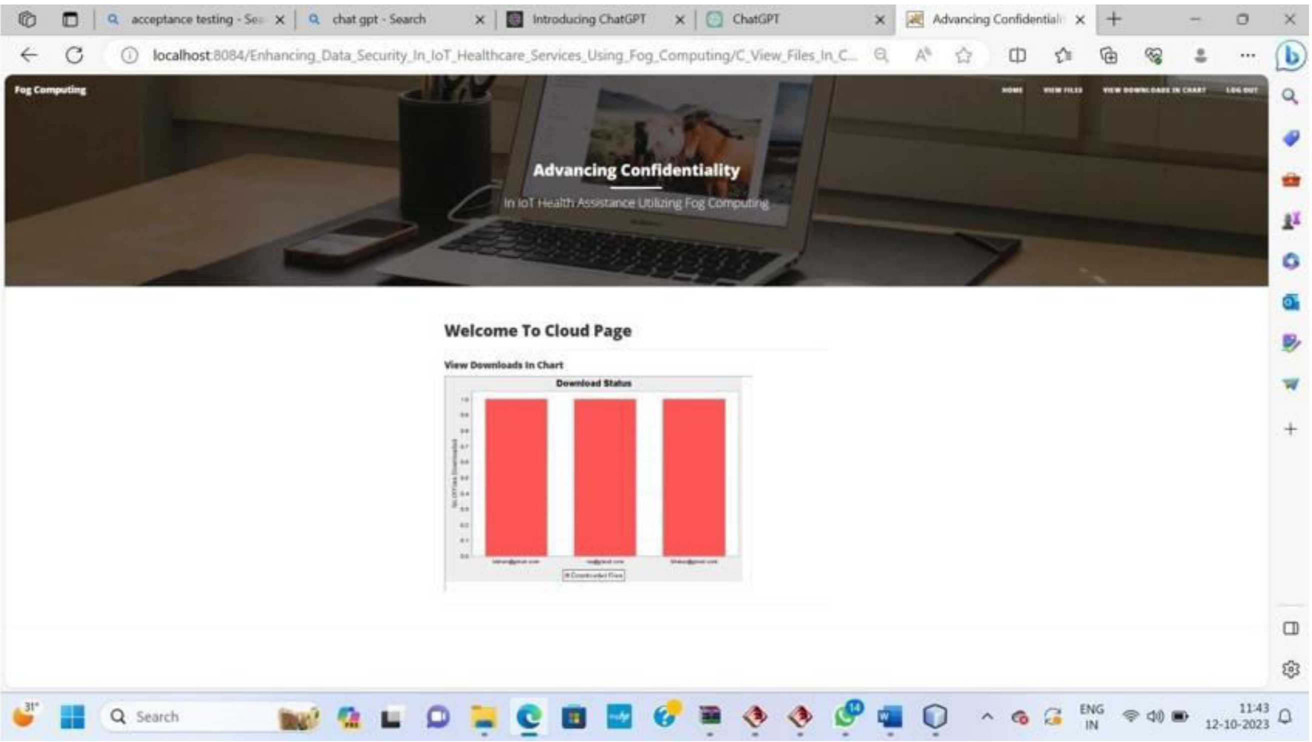


View All Uploaded Files into The Cloud

FILE ID	FILE NAME	DATA	UPLOAD DATE	STATUS
61153	sample.txt	this is the sample file	2020-03-08 06:52:50	uploaded_to_cloud
80141	a	hai this is file	2023-08-07 12:10:23	uploaded_to_cloud

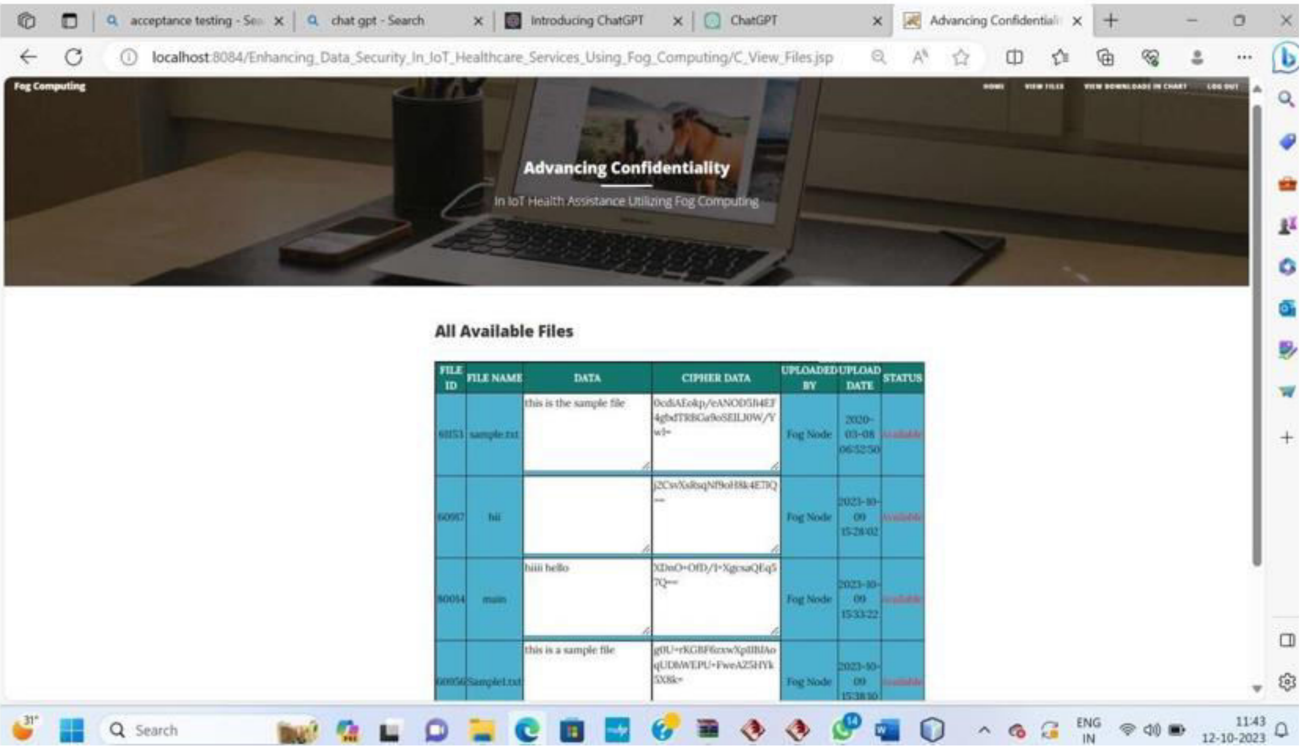
CLOUD LOGIN

A "cloud page login" typically refers to the login page or authentication interface for a web application or service that is hosted on the cloud. It's the webpage where users are required to enter theircredentials, such as a username and password, to access the cloud-based service.



Welcome To Cloud Page

View Downloads In Chart


acceptance testing - Search
chat gpt - Search
Introducing ChatGPT
ChatGPT
Advancing Confidentiali
localhost:8084/Enhancing_Data_Security_In_IoT_Healthcare_Services_Using_Fog_Computing/C_View_Files.jsp
Fog Computing
HOME
VIEW FILES
VIEW DOWNLOADS IN CHART
LOG OUT
Advancing Confidentiality
In IoT Health Assistance Utilizing Fog Computing
Search
ENG IN
11:43
12-10-2023

All Available Files

FILE ID	FILE NAME	DATA	CIPHER DATA	UPLOADED BY	UPLOAD DATE	STATUS
68153	sample.txt	this is the sample file	0cdiAEokp/eANOD5H4EF4gbdTRBGa9oSEILJ0W/Yw1=	Fog Node	2020-03-08 06:52:50	Available
60987	hii		j2CsvXs8sqNf9oH8k4E7IQ==	Fog Node	2023-10-09 15:28:02	Available
80014	main	hiiii hello	XDnO+OfD/I+XgcsaQEq57Q==	Fog Node	2023-10-09 15:33:22	Available
60956	Sample1.txt	this is a sample file	g0U+rKGBF6zxwXpIIBIAoqUD8WEPU+FweAZ5HYk5X8k=	Fog Node	2023-10-09 15:38:10	Available

CONCLUSION

Fog computing architecture is able to overcome the security challenges of the traditional IoT cloudarchitecture to some extent. By introducing fog as a middle layer and performing at the edge side it enhances data security, accuracy, consistency, reduces the latency rate and enhances the overall qualityof service. In the near future IoT-Fog-cloud architecture will be widely used as more and more IoT devices are developed and the increasing demand for fast computation. The implementation can be enhanced in future by developing a reliable real time data monitoring system application with the mentioned architecture as a core. And to give a computational prove of how much fog can enhance the traditional IoTCloud architecture.

FUTURE WORK

Fog computing architecture is able to overcome the security challenges of the traditional IoT cloudarchitecture to some extent. By introducing fog as a middle layer and performing at the edge side it enhances data security, accuracy, consistency, reduces the latency rate and enhances the overall qualityof service. In the near future IoT-Fog-cloud architecture will be widely used as more and more IoT devices are developed and the increasing demand for fast computation. The implementation can be enhanced in future by developing a reliable real time data monitoring system application with the mentioned architecture as a core. And to give a computational prove of how much fog can enhance the traditional IoTCloud architecture.

REFERENCES

1. Al Hamid, Hadeal Abdulaziz, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, and Atif Alamri. "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography." IEEE Access 5 (2017): 22313-22328.

2. Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. "Fog computing for the internet of things: Security and privacy issues." IEEE Internet Computing 21, no. 2 (2017): 34-42.

3. Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance evaluation of symmetric encryption algorithms." IJCSNS International Journalof Computer Science and Network Security 8, no. 12 (2008): 280- 286.

4. Coppersmith, Don, Donald Byron Johnson, and Stephen M. Matyas. "A proposed mode for triple-DES encryption." IBM Journal of Research and Development 40, no. 2 (1996): 253-262.

5. 10.Vishwanath, Akhilesh, Ramya Peruri, and Jing (Selena) He. Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.

6. Mukherjee, Mithun, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, and Vikas Kumar. "Security and privacy in fog computing: Challenges." IEEE Access 5 (2017): 19293- 19304.

7. Shrestha, N. M., Abeer Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi. "Enhancede-health framework for security and privacy in healthcare system." In Digital Information Processing and Communications (ICDIPC), 2016 Sixth International Conference on, pp. 75-79. IEEE, 2016.

8. Wang, Qixu, Dajiang Chen, Ning Zhang, Zhe Ding, and Zhiguang Qin. "PCP: A PrivacyPreserving Content-Based Publish–Subscribe Scheme With Differential Privacy in Fog Computing." IEEE Access 5 (2017): 17962- 17974.

9. Wanve, Balu, Rahul Kamble, Sachin Patil, and Jayshree Katti. "Framework for client side AES encryption technique in cloud computing." In Advance Computing Conference (IACC), 2015 IEEEInternational, pp. 525-528. IEEE, 2015.

10. Vishwanath, Akhilesh, Ramya Peruri, and Jing (Selena) He. Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.