Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography

Asi Muni Sekhar

Department of Computer Science, Sri Venkateswara University, Tirupati

Abstract— *Organizations share an evolving interest in adopting a cloud computing approach for Internet of Things (IoT) applications. Integrating IoT devices and cloud computing technology is considered as an effective approach to storing and managing the enormous amount of data generated by various devices. However, big data security of these organizations presents a challenge in the IoT–cloud architecture. To overcome security issues, we propose a cloud-enabled IoT environment supported by multifactor authentication and lightweight cryptography encryption schemes to protect big data system. The proposed hybrid cloud environment is aimed at protecting organizations' data in a highly secure manner. The hybrid cloud environment is a combination of private and public cloud. Our IoT devices are divided into sensitive and nonsensitive devices. Sensitive devices generate sensitive data, such as healthcare data; whereas nonsensitive devices generate nonsensitive data, such as home appliance data. IoT devices send their data to the cloud via a gateway device. Herein, sensitive data are split into two parts: one part of the data is encrypted using RC6, and the other part is encrypted using the Fiestel encryption scheme. Nonsensitive data are encrypted using the Advanced Encryption Standard (AES) encryption scheme. Sensitive and nonsensitive data are respectively stored in private and public cloud to ensure high security. The use of multifactor authentication to access the data stored in the cloud is also proposed. During login, data users send their registered credentials to the Trusted Authority (TA). The TA provides three levels of authentication to access the stored data: first-level authentication - read file, second-level authentication - download file, and third-level authentication - download file from the hybrid cloud. We implement the proposed cloud–IoT architecture in the NS3 network simulator. We evaluated the performance of the proposed architecture using metrics such as computational time, security strength, encryption time, and decryption time.*

***Keywords: Big Data, Cloud computing, Internet of Things, Multilevel authentication, Lightweight Cryptography*.**

I. INTRODUCTION

In accordance with the advancement and wide use of Internet of Things (IoT) applications and with the emergence of wireless communication and mobile technologies, IoT and cloud computing have become important concepts. IoT aims to provide connectivity for anything with minimum storage and computing capabilities. Security is a major issue in cloud-integrated IoT, and the user data stored in the cloud requires secure protection. A lightweight multifactor secured smart card-based user authentication is introduced in cloud–IoT applications. shows the architecture for cloud-integrated IoT, which consists of the hybrid cloud, IoT devices, and users. The hybrid cloud includes public and private cloud. The public cloud is used to store non sensitive data, whereas the private cloud is used to store highly sensitive data.

1.1 Cyber Security

Cybersecurity is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security.

It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as **information technology security**.

We can also define cybersecurity as the set of principles and practices designed to protect our computing resources and online information against threats. Due to the heavy dependency on computers in a modern industry that store and transmit an abundance of confidential and essential information about the people, cybersecurity is a critical function and needed insurance of many businesses.

1.2 Cyber Security Goals

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the **AIC (Availability, Integrity, and Confidentiality)** triad to avoid the confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

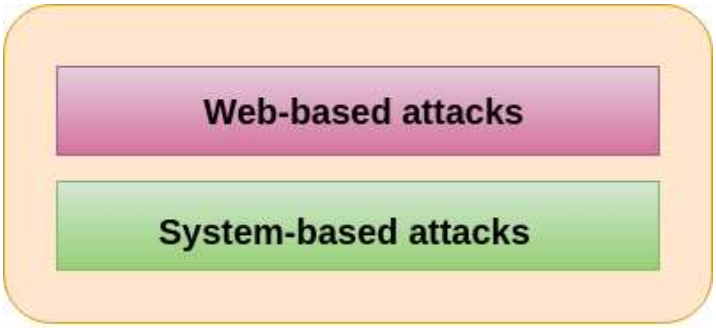
The CIA criteria are one that most of the organizations and companies use when they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of these security goals must come into effect. These are security policies that all work together, and therefore it can be wrong to overlook one policy.

1.3 Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

1.4 Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1.4.1 Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

1.4.2 DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

1.4.3 Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

1.4.4 Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

1.4.5 Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

1.4.6 Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

1.4.7 Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

1.4.8 URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

1.4.9 File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

1.4.10 Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

1.5 System-based attacks

these are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1.5.1 Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

1.5.2 Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

1.5.3 Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

1.5.4 Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

1.5.5 Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

1.6 Cyber Security Challenges

Today cybersecurity is the main component of the country's overall national security and economic security strategies. In India, there are so many challenges related to cybersecurity. With the increase of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured. These security analysts face many challenges related to cybersecurity such as securing confidential data of government organizations, securing the private organization servers, etc.

The recent important cybersecurity challenges are described below:

Cyber Security Challenges

1.6.1 Ransomware Evolution

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cybersecurity, data professionals, IT, and executives. Ransomware attacks are growing day by day in the areas of cybercrime.

IT professionals and business leaders need to have a powerful recovery strategy against the malware attacks to protect their organization. It involves proper planning to recover corporate and customers' data and application as well as reporting any breaches against the Notifiable Data Breaches scheme. Today's DRaaS solutions are the best defence against the ransomware attacks. With DRaaS solutions method, we can automatically back up our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

1.6.2 Blockchain Revolution

Blockchain technology is the most important invention in computing era. It is the first time in human history that we have a genuinely native digital medium for peer-to-peer value exchange. The blockchain is a technology that enables cryptocurrencies like Bitcoin. The blockchain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust.

It is difficult to predict what blockchain systems will offer in regards to cybersecurity. The professionals in cybersecurity can make some educated guesses regarding blockchain. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches.

1.6.3 IoT Threats

IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks.

When IoT things were designed, it is not considered in mind about the used in cybersecurity and for commercial purposes. So every organization needs to work with cybersecurity professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the risk.

1.6.4 AI Expansion

AI short form is Artificial intelligence. According to John McCarthy, father of Artificial Intelligence defined AI: "The science and engineering of making intelligent machines, especially intelligent computer programs."

It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include speech recognition, Learning, Planning, Problem-solving, etc. The key benefits with AI into our cybersecurity strategy has the ability to protect and defend an environment when the malicious attack begins, thus mitigating the impact. AI take immediate action against the malicious attacks at a moment when a threats impact a business. IT business leaders and cybersecurity strategy teams consider AI as a future protective control that will allow our business to stay ahead of the cybersecurity technology curve.

1.6.5 Serverless Apps Vulnerability

Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc. The serverless apps invite the cyber attackers to spread threats on their system easily because the users access the application locally or off-server on their device. Therefore it is the user responsibility for the security precautions while using serverless application.

The serverless apps do nothing to keep the attackers away from our data. The serverless application doesn't help if an attacker gains access to our data through a vulnerability such as leaked credentials, a compromised insider or by any other means then serverless.

We can run software with the application which provides best chance to defeat the cybercriminals. The serverless applications are typically small in size. It helps developers to launch their applications quickly and easily. They don't need to worry about the underlying infrastructure. The web-services and data processing tools are examples of the most common serverless apps.

II. LITERATURE REVIEW

1. Author: Geeta Sharma, Sheetal Kalra

Title: "A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services,"

Description: With the ongoing revolution of cloud computing and Internet of Things, remote patient monitoring has become feasible. These networking paradigms are widely used to provide healthcare services and real-time patient monitoring. The sensors that are either wearable or embedded within the body of a patient transmit patient's data to the remote medical centers. The medical professional can access patient's data stored in the cloud anywhere across the globe. As the sensitive data of the patient are sent over insecure cloud-IoT networks, secure user authentication is of utmost importance. An efficient user authentication scheme ensures that only legitimate users can access data and services. This paper proposes a secure and efficient user authentication scheme for remote patient monitoring. The proposed scheme is robust, lightweight and secure against multiple security attacks. Furthermore, the scheme has low computational overhead. A formal verification using AVISPA tool confirms the security of the proposed scheme.

2. Author: Geeta Sharma, Sheetal Kalra 2019

Title: Advanced Lightweight Multi-Factor Remote User Authentication Scheme for Cloud-IoT Applications,"

Description: With the ongoing revolution of Internet-enabled devices, Internet ofThings (IoT) has emerged as the most popular networking paradigm. The enormous amount of data generated from smart devices in IoT environment is one of the biggest concerns. Cloud computing has emerged as a key technology to process the generated data. The confidential data of user from IoT devices is stored in cloud server and the remote user can access this data anytime, anywhere and at any place from the cloud server. This makes remote user authentication a critical issue. This paper proposes a lightweight remote user authentication scheme for cloud-IoT applications. The formal security analysis using BAN logic and random oracle model confirms that the scheme is resilient to known security attacks. Furthermore, the scheme is formally verified using AVISPA tool which confirms the security against multiple security attacks.

3. Author: Chandrakar P, Om H 2019

Title: An efficient two-factor remote user authentication and session key agreement scheme using rabin cryptosystem

Description: In this paper, we present a safe and reliable remote user authentication and session key agreement scheme using the Rabin cryptosystem. The Rabin cryptosystem relies on prime integer factorization, which provides high security. Our scheme is validated using the Burrows–Abadi–Needham logic, which proved that it facilitates mutual authentication and session key agreement securely. The informal security analysis shows that the proposed scheme is secured against various malicious attacks. We simulate our scheme using the well-known Automated Validation of Internet Security Protocols and Applications tool, which confirms that the proposed scheme can defend from the passive and active attacks and also prevents the man-in-the-middle and replay attacks. Further, the performance evaluation shows that our scheme provides robustness against various security attacks as well as efficient in the terms of smart card storage cost, estimated execution time, communication cost and computation cost.

4. Author: Yoon, E.-J.; Ryu, E.-K.; Yoo, K.-Y 2004

Title: Further improvement of an efficient password based remote user authentication scheme using smart cards

Description: Recently, Ku-Chen proposed an improvement to Chien et al.'s scheme to prevent from some weaknesses. However, the improved scheme is not only still susceptible to parallel session attack, but also insecure for changing the user's password in password change phase. Accordingly, the current paper presents an enhancement to resolve such problems. As a result, the proposed scheme enables users to change their passwords freely and securely without the help of a remote server, while also providing secure mutual authentication1 .

5. Author: H.Y. Chien, J. K. Jan and Y.M. Tseng 2002

Title: An efficient and practical solution to remote authentication: smart card,"

Description: The smart card-based scheme is a very promising and practical solution to remote authentication. Compared with other smart card-based schemes, our solution achieves more functionality and requires much less computational cost. These important merits include: (1) there is no verification table; (2) users can freely choose their passwords; (3) the communication cost and the computational cost is very low; and (4) it provides mutual authentication between the user and the serve

III. EXISTING SYSTEM

Integrating IoT devices and cloud computing technology is considered as an effective approach to storing and managing the enormous amount of data generated by various devices. However, big data security of these organizations presents a challenge

in the IoT–cloud architecture. To overcome security issues, Security is a major issue in cloud-integrated IoT, and the user data stored in the cloud requires secure protection. A lightweight multifactor secured smart card-based user authentication is introduced in cloud IOT. IoT aims to provide connectivity for anything with minimum storage and computing capabilities. Security is a major issue in cloud-integrated IoT, and the user data stored in the cloud requires secure protection. A lightweight multifactor secured smart card-based user authentication is introduced in cloud–IoT applications. the architecture for cloud-integrated IoT, which consists of the hybrid cloud, IoT devices, and users. The hybrid cloud includes public and private cloud. The public cloud is used to store non sensitive data, whereas the private cloud is used to store highly sensitive data.

3.1 DISADVANTAGES

- The security of this method is not properly.
- It has large data so the computational is less
- The performance and the effectiveness is less

IV. PROPOSED SYSTEM

The proposed hybrid cloud environment is aimed at protecting organizations' data in a highly secure manner. The hybrid cloud environment is a combination of private and public cloud. Our IoT devices are divided into sensitive and nonsensitive devices. Sensitive devices generate sensitive data, such as healthcare data; whereas nonsensitive devices generate nonsensitive data, such as home appliance data. IoT devices send their data to the cloud via a gateway device. Herein, sensitive data are split into two parts: one part of the data is encrypted using RC6, and the other part is encrypted using the Fiestel encryption scheme. Nonsensitive data are encrypted using the Advanced Encryption Standard (AES) encryption scheme. Sensitive and nonsensitive data are respectively stored in private and public cloud to ensure high security. The use of multifactor authentication to access the data stored in the cloud is also proposed. During login, data users send their registered credentials to the Trusted Authority (TA). The TA provides three levels of authentication to access the stored data: first-level authentication - read file, second-level authentication - download file, and third-level authentication - download file from the hybrid cloud. We implement the proposed cloud–IoT architecture in the NS3 network simulator. We evaluated the performance of the proposed architecture using metrics such as computational time, security strength, encryption time, and decryption time.

The main aim of the current work is to propose a multilevel authentication scheme that can provide enhanced security in an integrated IoT–cloud environment. The main contributions of this work are summarized as follows:

➢ It proposes a hybrid cloud consisting of private and public cloud that can improve the security of IoT systems. IoT devices are also divided into sensitive and nonsensitive devices on the basis of the type of data produced.

➢ The security of sensitive data from sensitive devices is ensured by encrypting them using RC6 and the Fiestel encryption scheme. The encrypted sensitive data are stored in a private cloud via a gateway device to provide high security.

➢Nonsensitive data from nonsensitive devices are encrypted through the AES algorithm and then stored in a public cloud via a gateway device.

➢ To protect cloud-stored data from malicious users, this work proposes a multilevel authentication scheme with trusted authority (TA). The multilevel authentication scheme is subdivided into three levels, however adding (TA) to the proposed Cloud-IoT Environment will result in extra cloud service cost, since the Environment will deal with third party service.

➢ To prevent malicious users from reading stored files, this work proposes a first-level authentication scheme. At this level, users need to provide their user ID and password to the TA. Then, the TA verifies these credentials against registered credentials. If the verification is successful, then the TA grants the users access to read the files; otherwise, it rejects the request for access.

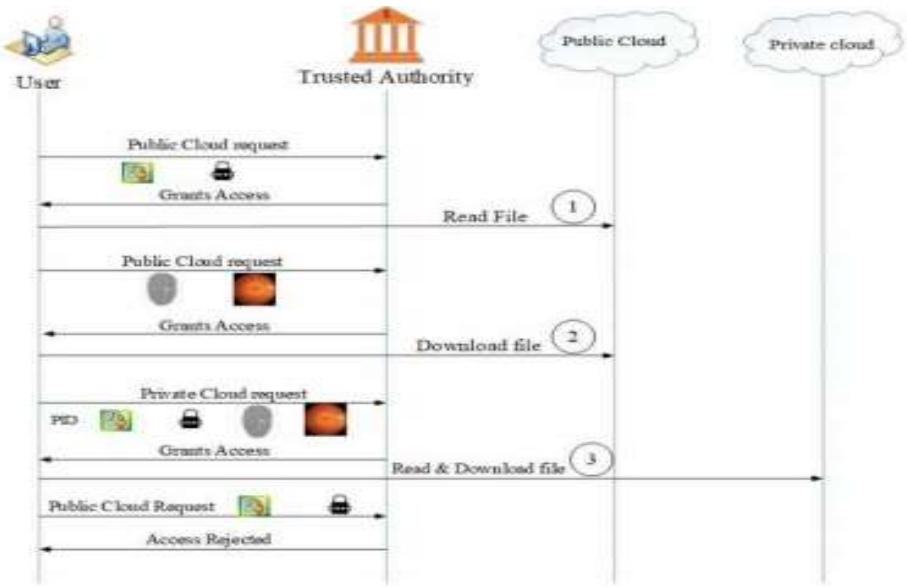
➢ To prevent unauthorized users from downloading files, this work provides a second-level authentication scheme in which users need to provide their biometrics, such as fingerprint and retina, to the TA. Then, the TA verifies the given credentials against registered credentials. If the verification is successful, then the TA grants the users access to download files; otherwise, it rejects the request for access.

➢ The final level of authentication is proposed to protect the data from unauthorized reading and downloading. At this level, users need to provide their user ID, password, and biometrics to the TA. Then, the TA verifies the given credentials against registered credentials. If the verification is successful, then the TA grants the users access to download and read the files from the cloud; otherwise, it rejects the request for access.

4.1 Advantages

- High security and more effective.
- The advantages of our scheme are proved for security performance, communication.

V. SYSTEM ARCHITECTURE



VI. APPLICATION AND THE FUTURE ENHANCEMENT

The cloud-integrated IoT applications have become popular among researchers due to their vital applications in organizations, private sectors, domestic appliances, etc.

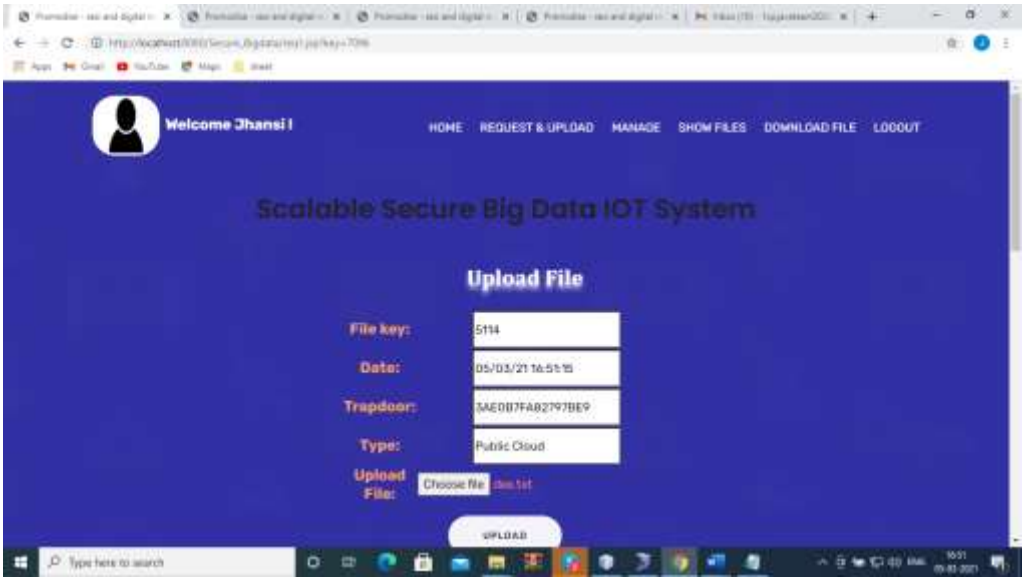
In the future, we intend to propose mutual authentication between gateway devices and IoT devices. In addition, we aim to propose DDoS attack detection in cloud servers.

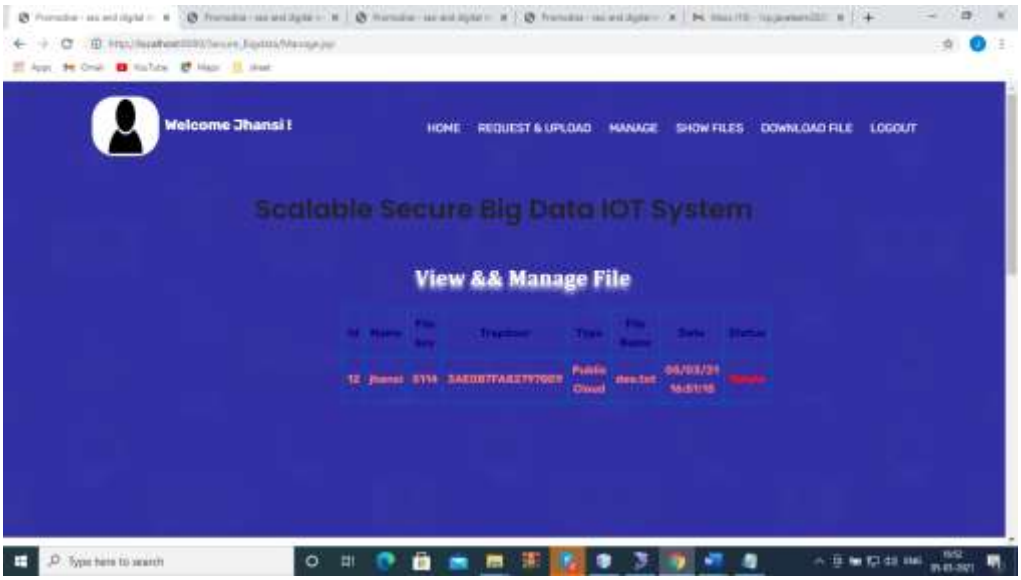
Home:

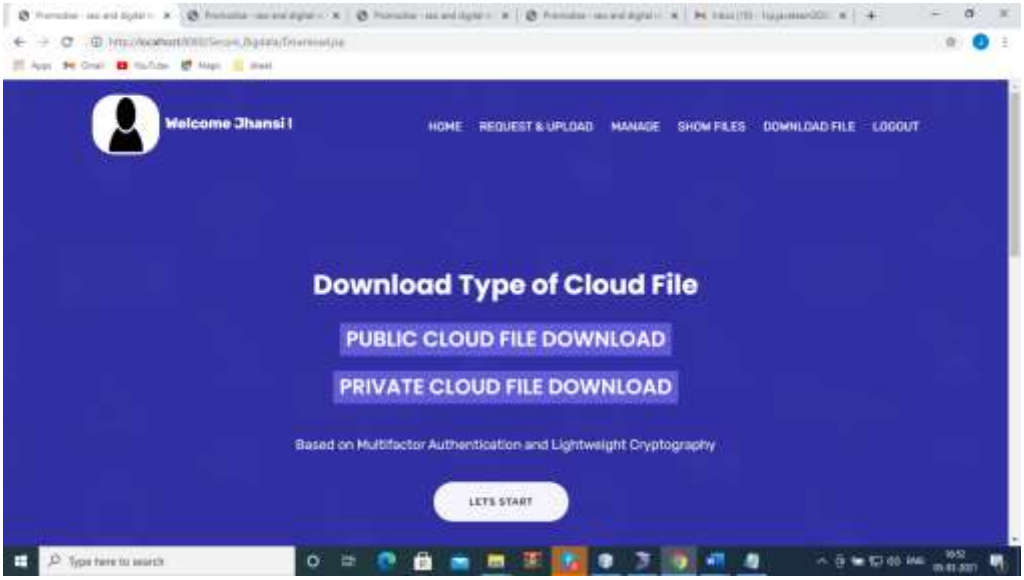
User:


Welcome Jhansi !
HOME
REQUEST & UPLOAD
MANAGE
SHOW FILES
DOWNLOAD FILE
LOGOUT
INFORMATION FORENSICS AND SECURITY
Scalable Secure Big Data IOT System
Based on Multifactor Authentication and Lightweight Cryptography
LETS START

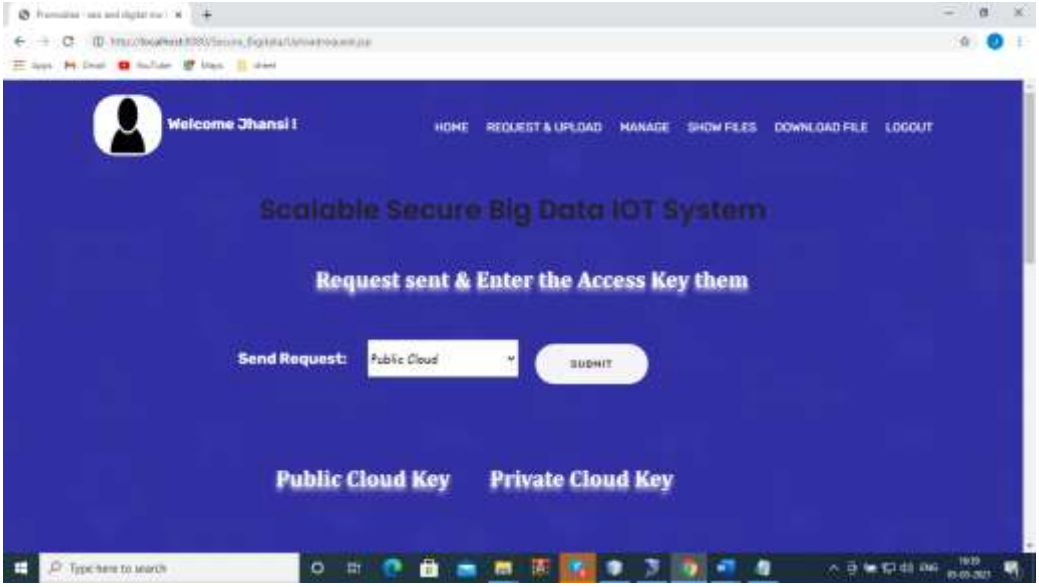

Welcome Jhansi !
HOME
REQUEST & UPLOAD
MANAGE
SHOW FILES
DOWNLOAD FILE
LOGOUT
Scalable Secure Big Data IOT System
Request sent & Enter the Access Key them
Send Request:
Public Cloud
SUBMIT
Public Cloud Key
Private Cloud Key


Welcome Jhansi !
HOME
REQUEST & UPLOAD
MANAGE
SHOW FILES
DOWNLOAD FILE
LOGOUT
Scalable Secure Big Data IOT System
Upload File
File key:
5114
Date:
05/03/21 16:51:15
Trapdoor:
3AE0B7FA82797BE9
Type:
Public Cloud
Upload File:
Choose file
UPLOAD



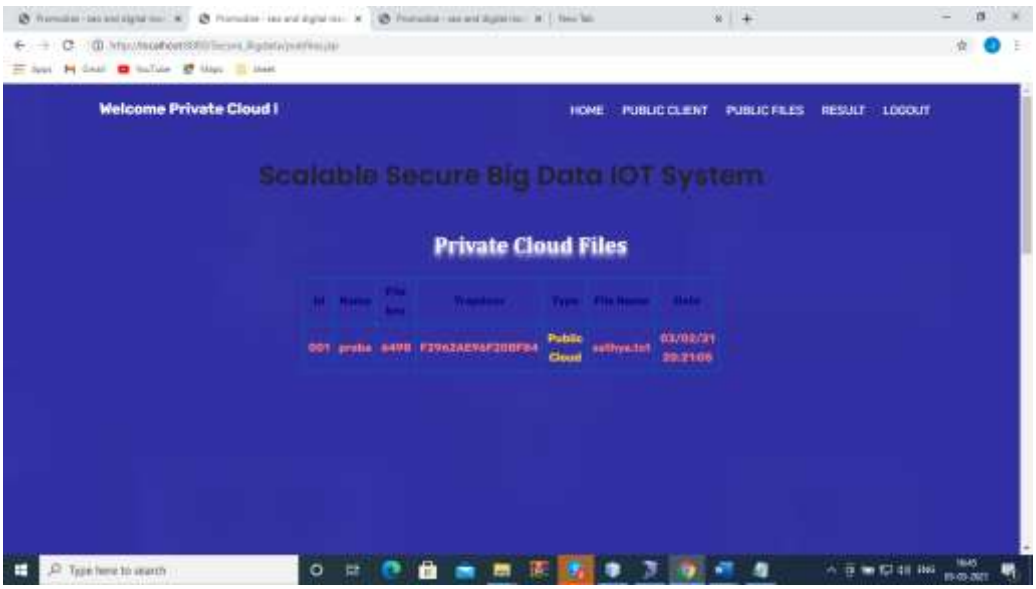


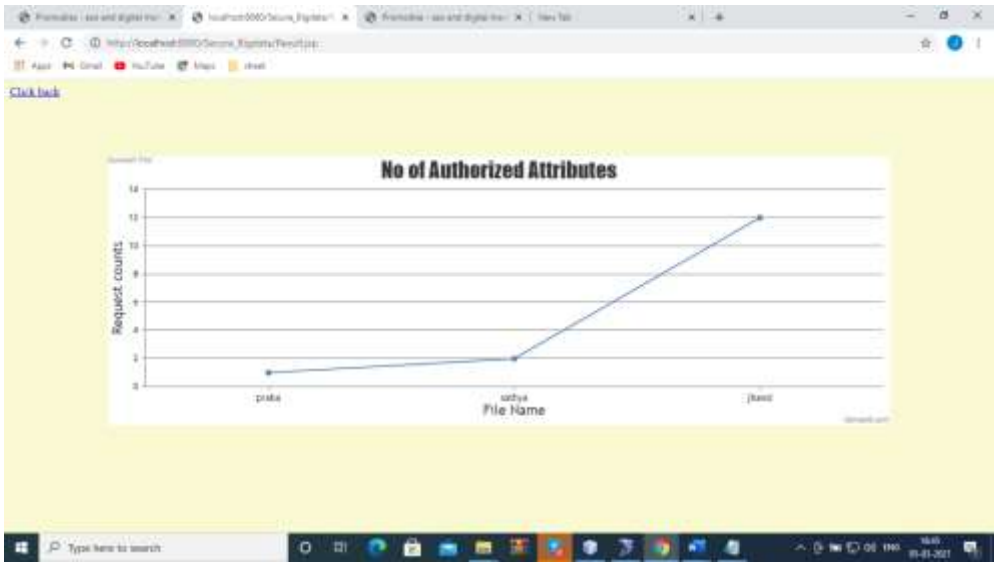
Public cloud




Welcome Trust Authority !
HOME
PUBLIC CLIENT
PUBLIC FILES
RESULT
LOGOUT
INFORMATION FORENSICS AND SECURITY
Scalable Secure Big Data IOT System
Based on Multifactor Authentication and Lightweight Cryptography
LETS START

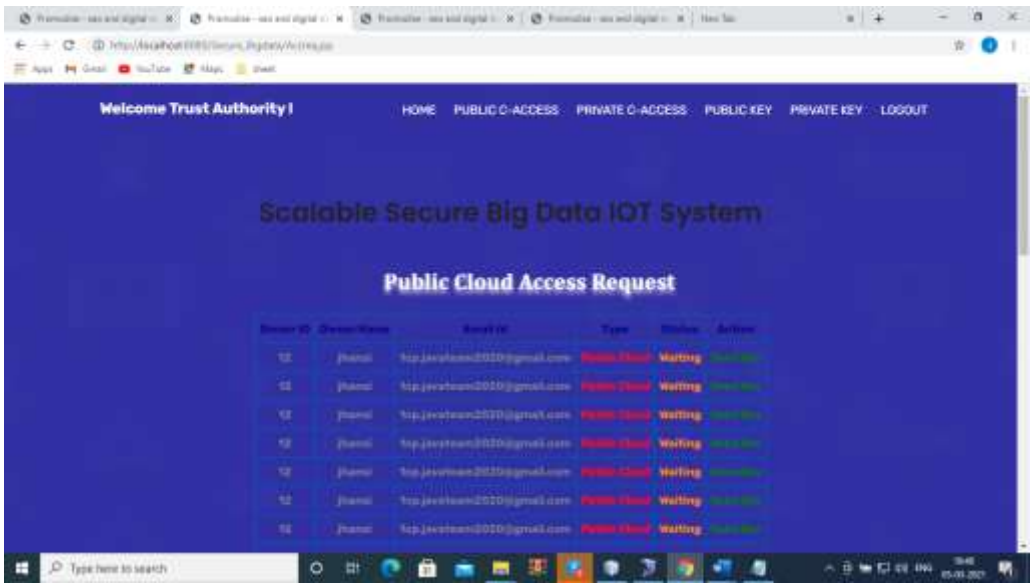

Welcome Private Cloud !
HOME
PUBLIC CLIENT
PUBLIC FILES
RESULT
LOGOUT
Scalable Secure Big Data IOT System
Public Cloud Clients

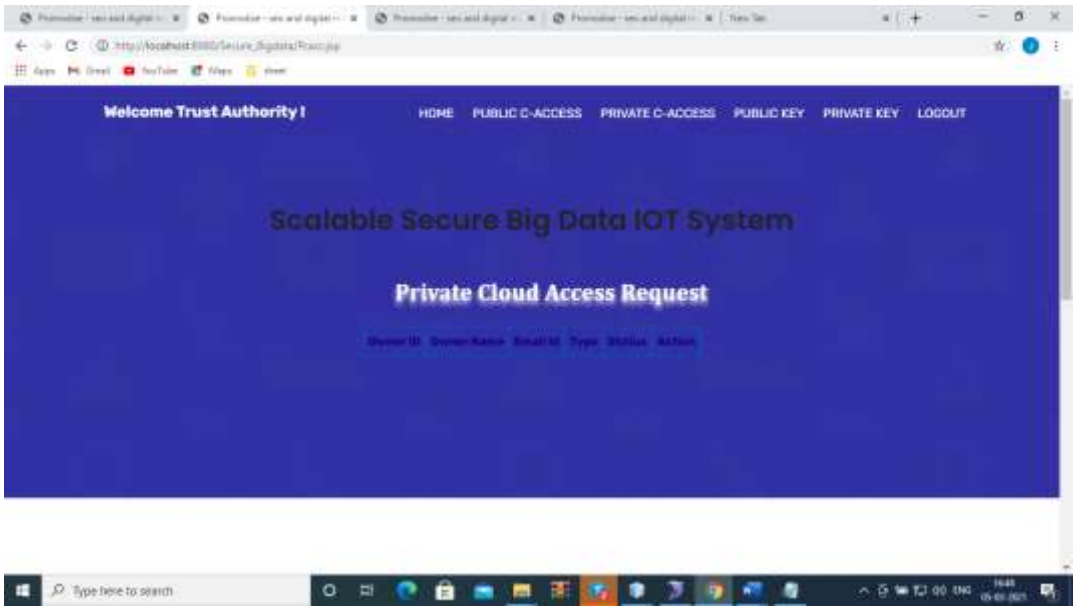

Welcome Private Cloud !
HOME
PUBLIC CLIENT
PUBLIC FILES
RESULT
LOGOUT
Scalable Secure Big Data IOT System
Private Cloud Files

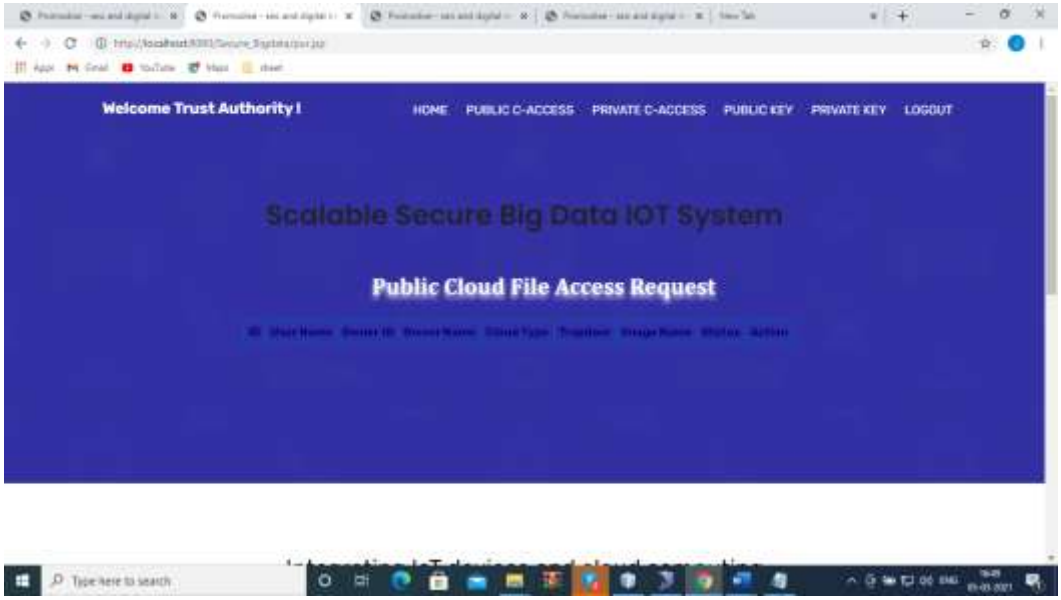

Click back
No of Authorized Attributes
Request counts
File Name

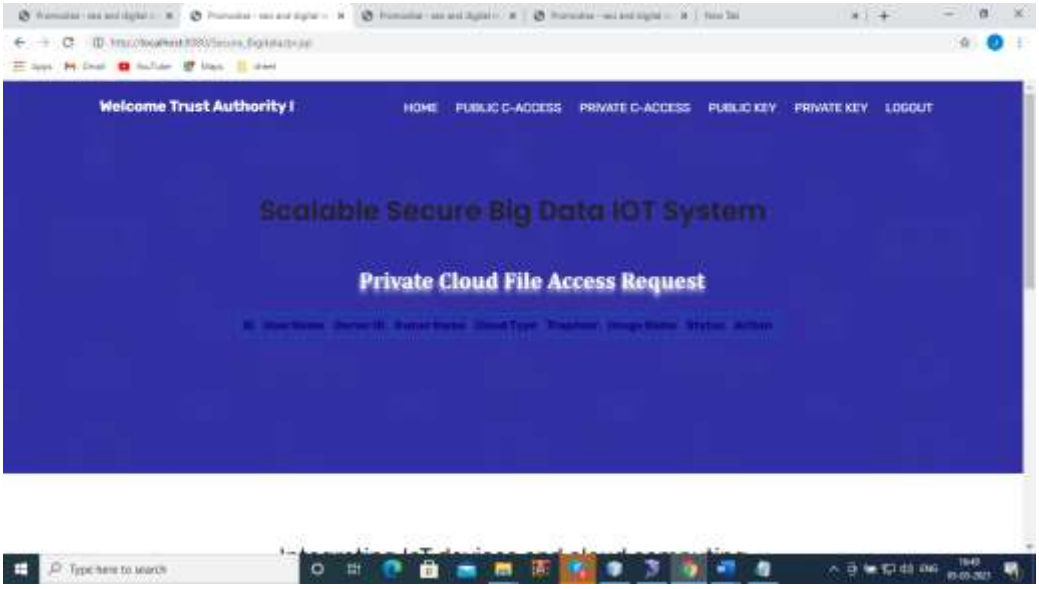
TA


Welcome Trust Authority I
HOME
PUBLIC C-ACCESS
PRIVATE C-ACCESS
PUBLIC KEY
PRIVATE KEY
LOGOUT
INFORMATION FORENSICS AND SECURITY
Scalable Secure Big Data IOT System
Based on Multifactor Authentication and Lightweight Cryptography
LETS START

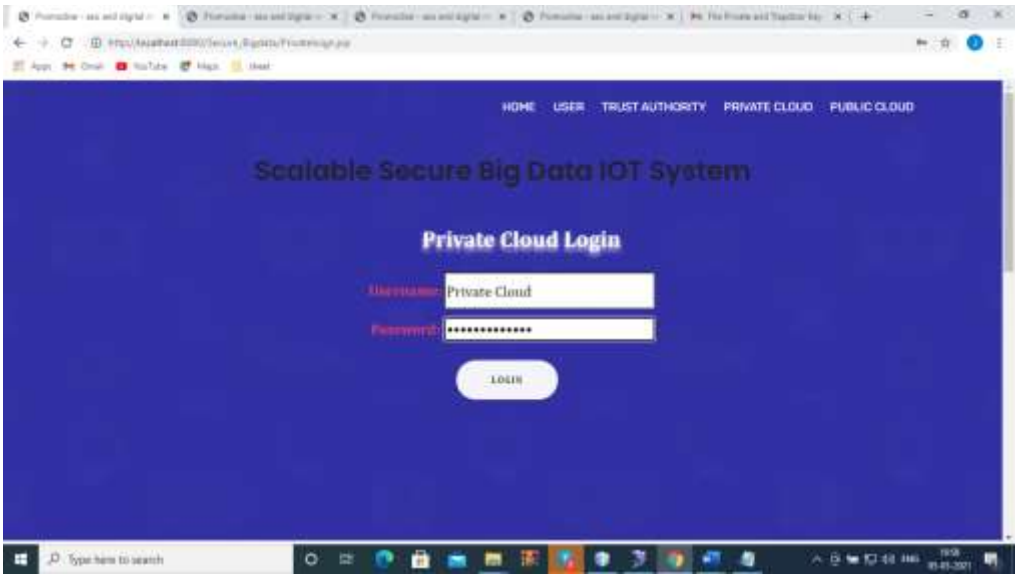

Welcome Trust Authority I
HOME
PUBLIC C-ACCESS
PRIVATE C-ACCESS
PUBLIC KEY
PRIVATE KEY
LOGOUT
Scalable Secure Big Data IOT System
Public Cloud Access Request

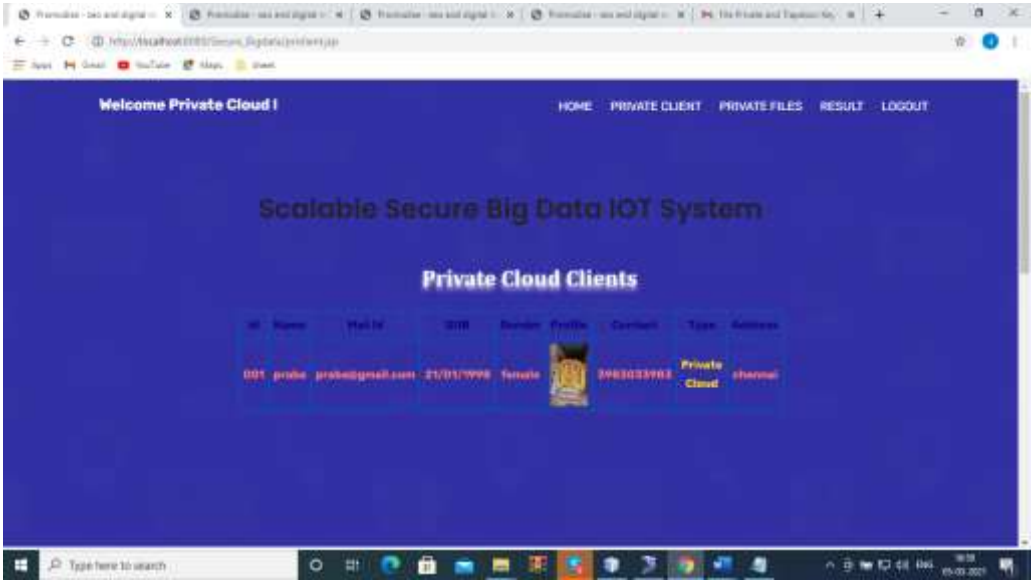

Welcome Trust Authority I
HOME
PUBLIC C-ACCESS
PRIVATE C-ACCESS
PUBLIC KEY
PRIVATE KEY
LOGOUT
Scalable Secure Big Data IOT System
Private Cloud Access Request

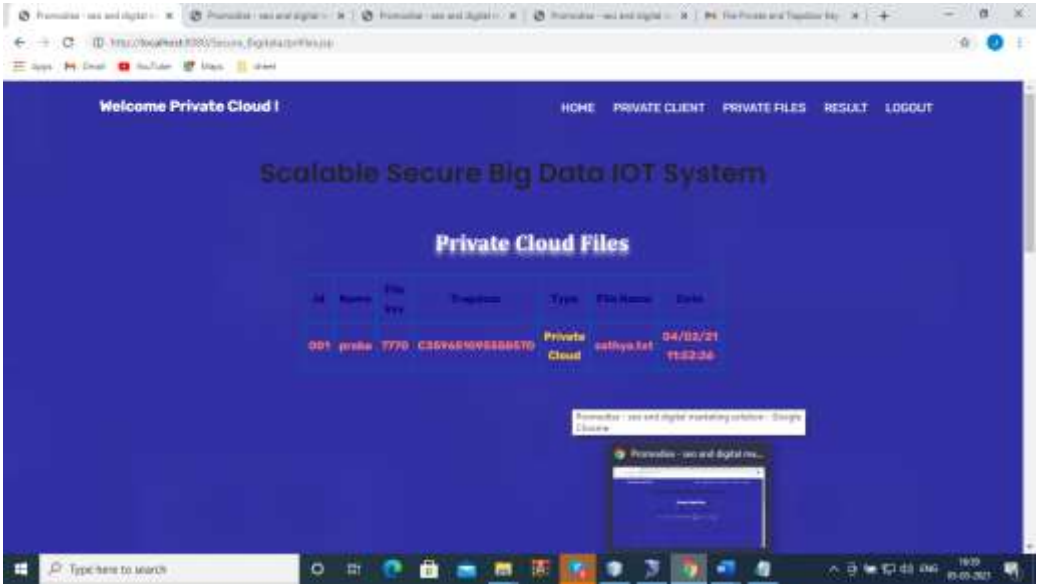

Welcome Trust Authority I
HOME
PUBLIC C-ACCESS
PRIVATE C-ACCESS
PUBLIC KEY
PRIVATE KEY
LOGOUT
Scalable Secure Big Data IOT System
Public Cloud File Access Request

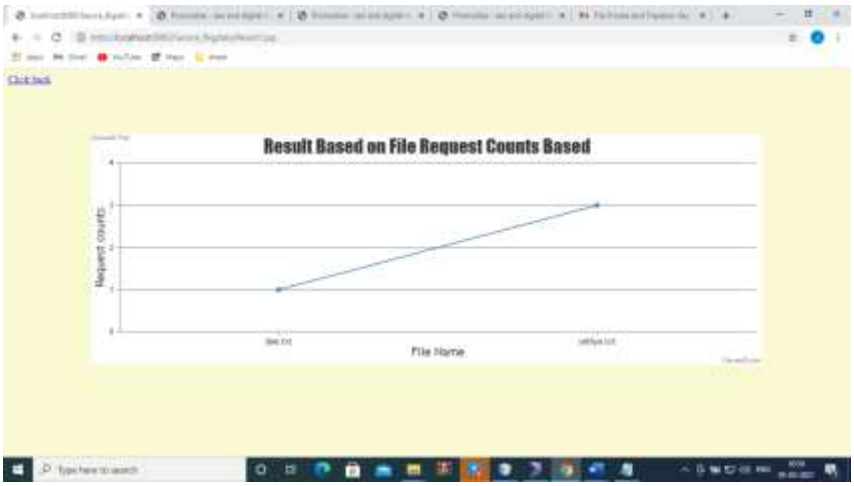

Welcome Trust Authority I
HOME
PUBLIC C-ACCESS
PRIVATE C-ACCESS
PUBLIC KEY
PRIVATE KEY
LOGOUT
Scalable Secure Big Data IOT System
Private Cloud File Access Request

Private cloud









VII. CONCLUSION

In recent years, cloud-integrated IoT applications have become popular among researchers due to their vital applications in organizations, private sectors, domestic appliances, etc. This work proposes a secure cloud–IoT environment using multifactor authentication and lightweight cryptography schemes. The proposed method splits IoT devices into sensitive and nonsensitive devices. We propose the use of a hybrid cloud that contains public cloud and private cloud. Sensitive device data are divided into two and encrypted using the RC6 and Fiestel encryption algorithms. These data are stored in a private cloud to provide high security via a gateway device. By contrast, nonsensitive device data are encrypted using AES and stored in a public cloud via a gateway device. Multifactor authentication is provided by the TA. In this process, the user undergoes three levels of authentication by providing their credentials, such as user ID, password, and biometrics (e.g., retina and fingerprint). We evaluate the performance of the proposed method using metrics that include computational time, security strength, encryption time, and decryption time. From the comparison results, we prove that the proposed method performs better than FCS, CP-ABE, and MCP-ABE.

REFERENCES

[1] Qinlong Huang, Licheng Wang, Yixian Yang, "DECENT: Secure And Fine-Grained Data Access Control With Policy Updating for Constrained IoT Devices," World Wide Web, Volume 21, Issue 1, pp. 151–167, 2018.

[2] Geeta Sharma, Sheetal Kalra, "A Lightweight Multi-Factor Secure Smart Card Based Remote User Authentication Scheme for Cloud-IoT Applications," Journal of Information Security and Applications, Volume 42, pp. 95–106, 2018.

[3] [5] Shahid Raza, Tómas Helgason, Panos Papadimitratos, Thiemo Voigt, "SecureSense: End-to-End Secure Communication Architecture for the Cloud-Connected Internet of Things," Future Generation Computer Systems, Volume 77, pp. 40–51, 2017.

[4] [6] Byung-Wook Jin, Jung-Oh Park, Hyung-Jin Mun, "A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment," Wireless Personal Communication, pp. 1–10, 2018.

[5] [7] Chen, "Collaboration IoT-Based RBAC With Trust Evaluation Algorithm Model for Massive IoT Integrated Application," Mobile Networks and Applications, pp. 1–14, 2018.

[6] [8] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, "Lightweight IoT-Based Authentication Scheme in Cloud Computing Circumstance," Future Generation Computer Systems, Volume 91, pp. 244–251, 2019.

[7] [9] Geeta Sharma, Sheetal Kalra, "Advanced Lightweight Multi-Factor Remote User Authentication Scheme for Cloud-IoT Applications," Journal of Ambient Intelligence and Humanized Computing, pp. 1–24, 2019.

[8] [10] Jia Guo, Ing-Ray Chen, Ding-Chau Wang, Jeffrey J. P. Tsai, Hamid Al-Hamadi, "Trust-Based IoT Cloud Participatory Sensing of Air Quality," Wireless Personal Communications, pp. 1–14, 2019.

[9] [11] Xiang Li, Xin Jin, Qixu Wang, Mingsheng Cao, Xingshu Chen, "SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context," Wireless Communications and Mobile Computing, Volume 2018, 2018.

[10] Zhitao Guan, Jing Li, Longfei Wu, Yue Zhang, Jun Wu, Xiaojiang Du, "Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid," IEEE Internet of Things Journal, Volume 4 , Issue 6, pp. 1934–1944, 2017.