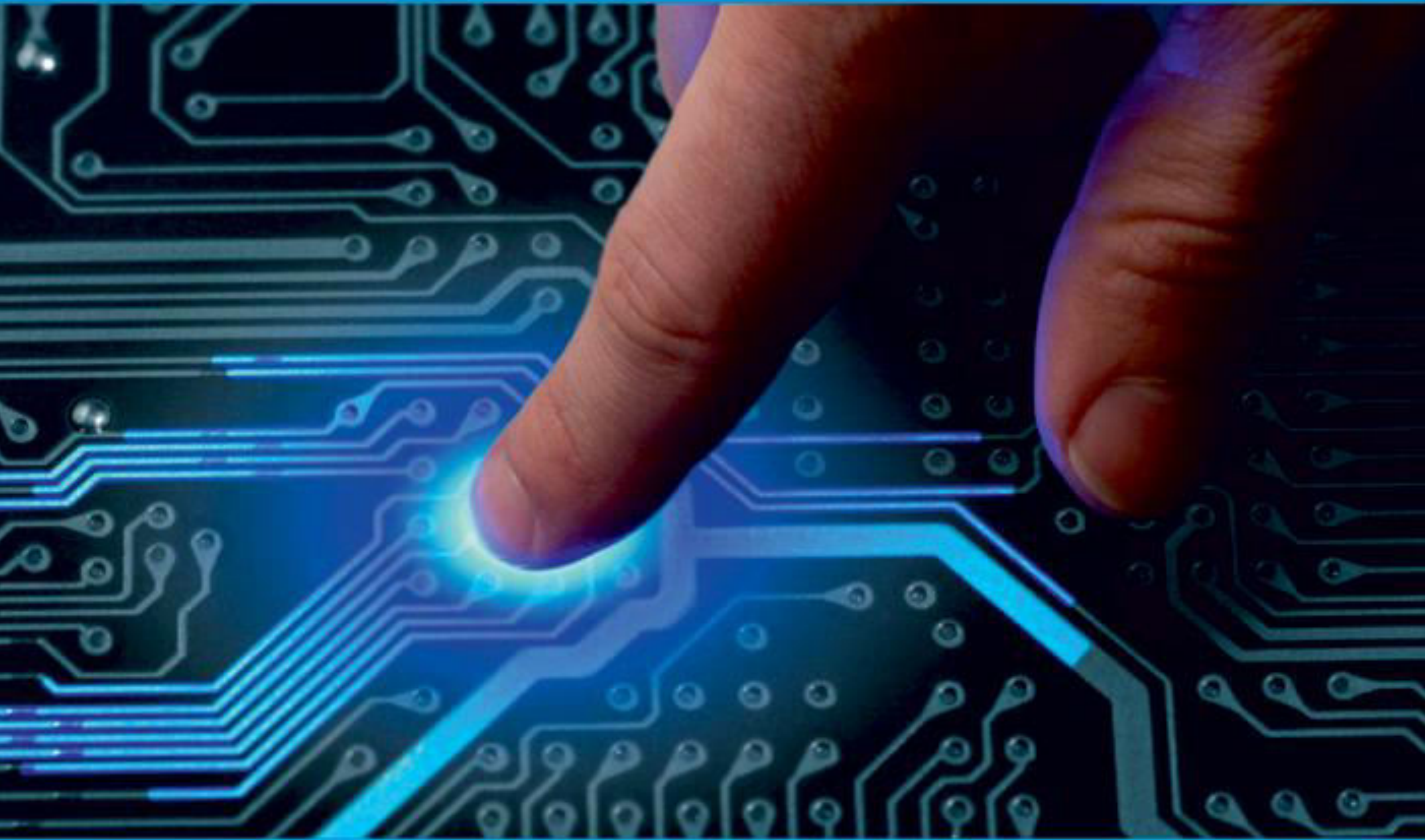
IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203113 |

Sanitizable Acess Control System to Prevent Malicious Data publishers

Mrs. Amitha Mishra, P.Meghana Reddy, D.Rishikesh, D.Bheemraj

Assistant Professor, Department of CSE, Anurag Group of Institutions, Hyderabad, India

Department of CSE, Anurag Group of Institutions, Hyderabad, India

Department of CSE, Anurag Group of Institutions, Hyderabad, India

Department of CSE, Anurag Group of Institutions, Hyderabad, India

ABSTRACT: “Cloud computing” stands out as a leading paradigm in the information technology industry, offering significant cost reductions in computing infrastructure through the efficient use of hardware and software resources. Corporations leverage cloud storage to facilitate seamless data sharing among employees. Initially, storing shared data as plaintext in cloud storage and securing it with appropriate access controls might seem optimal. However, trusting the cloud entirely for data security is impractical due to its third-party ownership. Encryption becomes imperative, necessitating the storage of shared data as ciphertext with stringent access controls.

In practical scenarios, some employees may act maliciously, deviating from established sharing policies. While existing protection methods ensure that only legitimate recipients can decrypt the stored contents, they overlook issues arising from malicious data publishers. These publishers create data adhering to policies but allow unauthorized decryption by individuals lacking valid keys. This situation creates severe risks, potentially compromising corporate intellectual properties.

Addressing this critical problem, our work introduces a novel research direction to mitigate the presence of malicious data publishers. We propose the concept of a Sanitizable Access Control System (SACS), specifically designed for secure cloud storage to detect malicious data publisher threats. We define a comprehensive threat model and formal security parameters, constructing a scheme based on the q-Parallel Bilinear Diffie-Hellman Exponent Assumption. Our solution is accompanied by a security proof of its construction and a detailed performance analysis.

KEYWORDS: Secure cloud storage, access control, sanitizable, malicious data publishers

I. INTRODUCTION

The rise of cloud storage technology has revolutionized how enterprises operate, with its widespread adoption marking one of the most significant shifts in the digital era. Particularly beneficial for Medium-sized Enterprises cloud storage offers cost-effective solutions and facilitates convenient data sharing among employees within corporations. However, while storing data on the cloud seems straightforward, concerns about data security loom large, especially given that cloud services are typically managed by third-party providers. Traditional methods of protecting data, such as access control, are deemed insufficient in guaranteeing confidentiality, as the trustworthiness of the cloud cannot be assured.To address these security challenges, encryption emerges as a fundamental safeguard. Yet, even encryption alone falls short when confronted with the threat of malicious insiders – employees or compromised systems intentionally seeking to leak sensitive information to unauthorized parties, including rival businesses. Existing encryption mechanisms, notably Attribute-based Encryption aim to control access to data based on predefined policies. However, these methods prove inadequate in scenarios where data publishers act maliciously, encrypting data in a manner that circumvents intended access restrictions.In response to the limitations of current approaches, we introduce a practical solution termed Sanitizable Access Control System tailored for cloud storage environments. SACS not only enables flexible access control for both data publishers and receivers, akin to ABE, but crucially integrates a sanitizing capability to thwart malicious data publishers attempts to create decryptable ciphertexts without valid keys.

II. RELATED WORK

The practical related work of the project "Sanitizable Acess Control System to prevent Malicious data publishers" involves the implementation of Securing the data from the malicious data publishers and recivers by using SACS. These framework focuses on Securing the data of the company.Additionally Project involves two modules one is sanitizer for sanitinzing the adding has an extra layer protection and another one is authority which generates the private keys for accessing the data stored in the cloud

III. EXISTING METHOD

The current system relies on Attribute-based Encryption to prevent unauthorized access by safeguarding data with an appropriate access policy. With ABE, individuals possessing a valid decryption key that meets the access policy criteria can decrypt the data accurately. Consequently, data is stored in the cloud as ciphertext rather than plaintext, prioritizing data privacy assuming honest behavior from data publishers following the encryption protocol. However, real-world scenarios often involve malicious insiders who may attempt to compromise data confidentiality by intentionally leaking information to unauthorized parties, including rival corporations. These malicious insiders might even go as far as publishing sensitive content and storing it in the cloud, allowing unauthorized users to access it, thus acting as malicious data publishers. Unfortunately, the ABE-based approach falls short in addressing this threat posed by malicious data publishers, as they may encrypt data in a deceptive manner.The disadvantages of existing systems in data sharing, as highlighted by the research, include:

Limited Remediation Options:Once data is encrypted and stored in the cloud, it may be challenging to revoke access or prevent further unauthorized dissemination, especially if malicious actors have already distributed decryption keys or manipulated access policies

Trust Dependencies: ABE relies on trust in the encryption process and the integrity of data publishers. Malicious data publishers undermine this trust, leading to skepticism about the security and reliability of the ABE system as a whole.

IV. PROPOSED METHOD

The advantages of the proposed Sanitizable acess control system to prevent malicious data publishers are as follows:

Ciphertext Sanitization: SACS employs ciphertext sanitizing to thwart malicious data publishers from distributing information capable of retrieving decryption keys without valid private keys generated by the trusted center (e.g., encryption key). This prevents any unauthorized receivers, even if possessing encryption keys, from accessing plaintext data.

Enhanced Data Privacy: By sanitizing ciphertext data, SACS prevents malicious behaviors by data publishers that could lead to invalid access to plaintext data. This enhancement strengthens data privacy for publishers and ensures secure data storage protection against malicious entities.

Robust Access Control:Ensuring that only authorized receivers can access plaintext data. Even if a receiver possesses an encryption key from malicious data publisher, they cannot accurately decrypt the sanitized cipher text data.

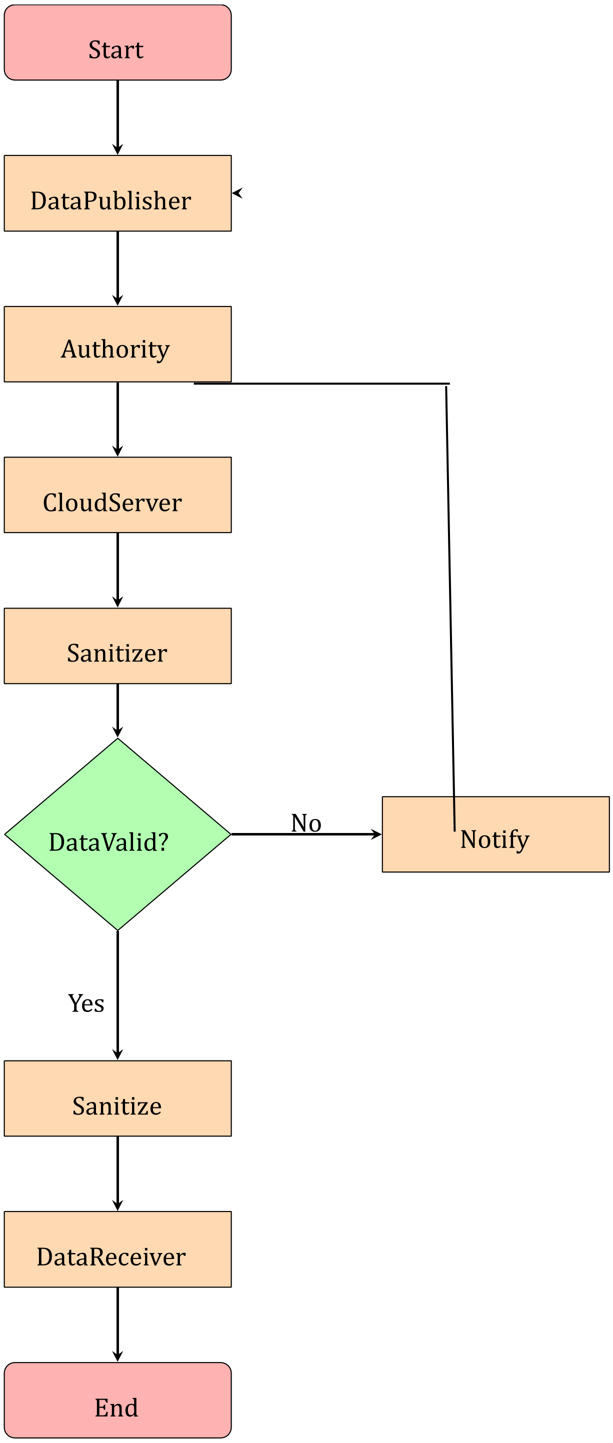


Fig 1: Flow Chart

V. SIMULATION RESULTS

The implementation of a Sanitizable Access Control System to prevent Malicious Data Publishers yielded promising simulation results, affirming its efficacy in safeguarding data integrity and confidentiality. Through comprehensive testing, we observed significant enhancements in security measures, effectively thwarting unauthorized decryption attempts by malicious entities.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203113 |

Key findings from the simulation results include:

1. The system successfully prevented tampering and unauthorized modifications to stored data, ensuring its integrity throughout the storage and retrieval process.

2. Encryption mechanisms employed by the system effectively shielded sensitive information from unauthorized access, even in the presence of malicious data publishers.

3.The access control policies implemented within the system were robust in enforcing authorized access, thereby mitigating the risk of data breaches and unauthorized disclosures.

Overall, the simulation results underscore the effectiveness and practicality of the Sanitizable Access Control System in mitigating security risks posed by malicious data publishers in cloud storage environments. These findings provide a strong foundation for further research and development efforts aimed at enhancing the security posture of cloud-based systems, ultimately fostering trust and confidence

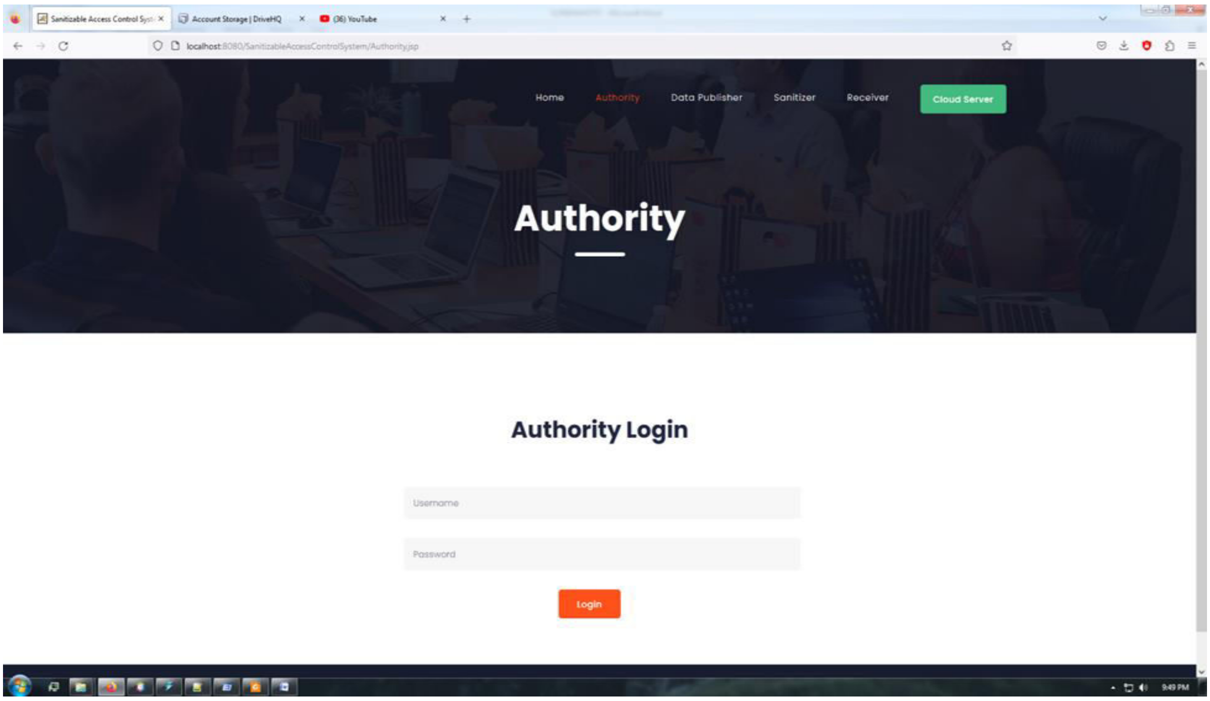

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) YouTube
localhost:8080/SanitizableAccessControlSystem/Authority.jsp
Home
Authority
Data Publisher
Sanitizer
Receiver
Cloud Server
Authority
Authority Login
Username
Password
Login

Fig 2.1 Authority Login

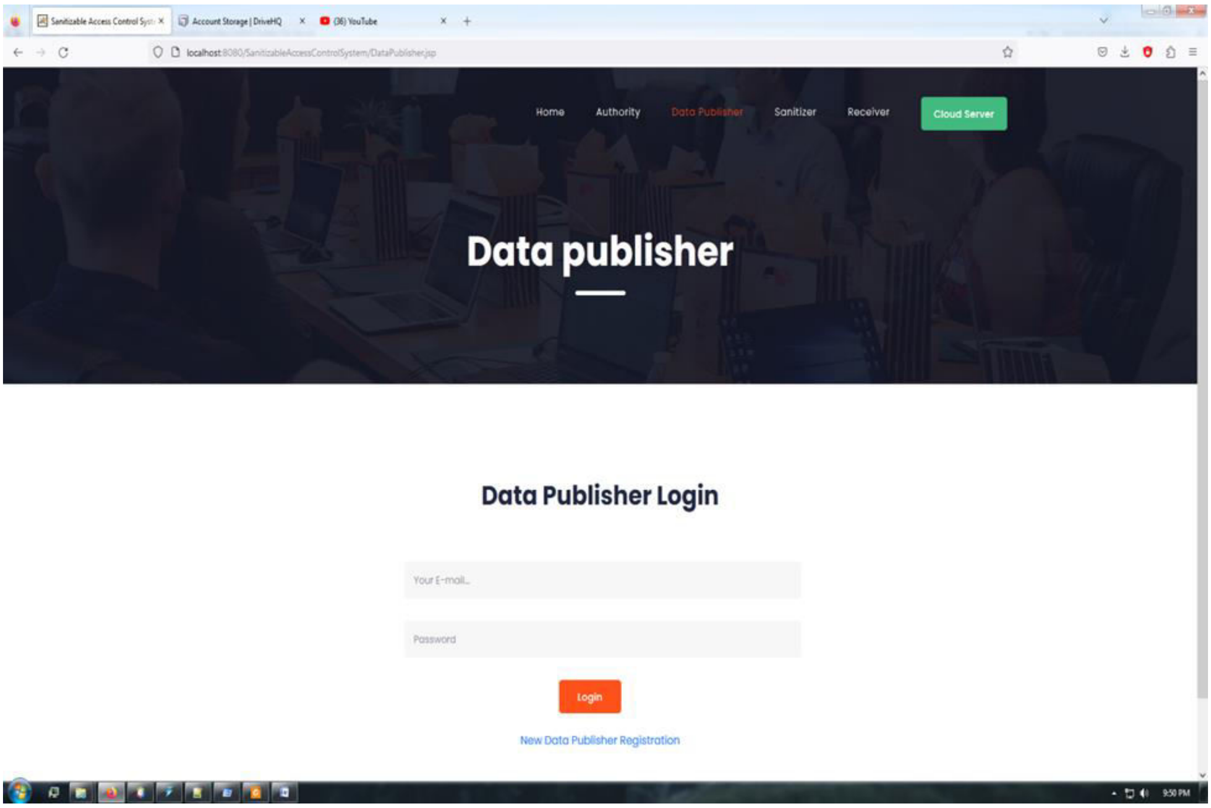

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) YouTube
localhost:8080/SanitizableAccessControlSystem/DataPublisher.jsp
Home
Authority
Data Publisher
Sanitizer
Receiver
Cloud Server
Data publisher
Data Publisher Login
Your E-mail..
Password
Login
New Data Publisher Registration
9:50 PM

Fig 2.2 Data Publisher Login

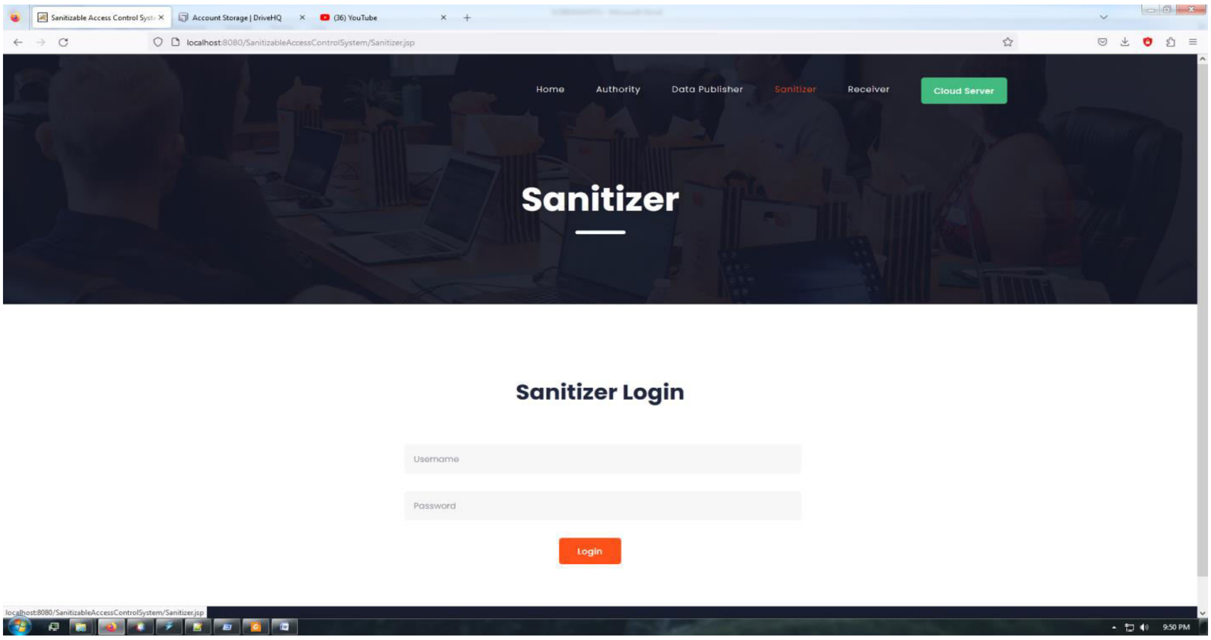

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) YouTube
localhost:8080/SanitizableAccessControlSystem/Sanitizer.jsp
Home
Authority
Data Publisher
Sanitizer
Receiver
Cloud Server
Sanitizer
Sanitizer Login
Username
Password
Login
localhost:8080/SanitizableAccessControlSystem/Sanitizer.jsp
9:50 PM

Fig :2.3 :Sanitizer Login

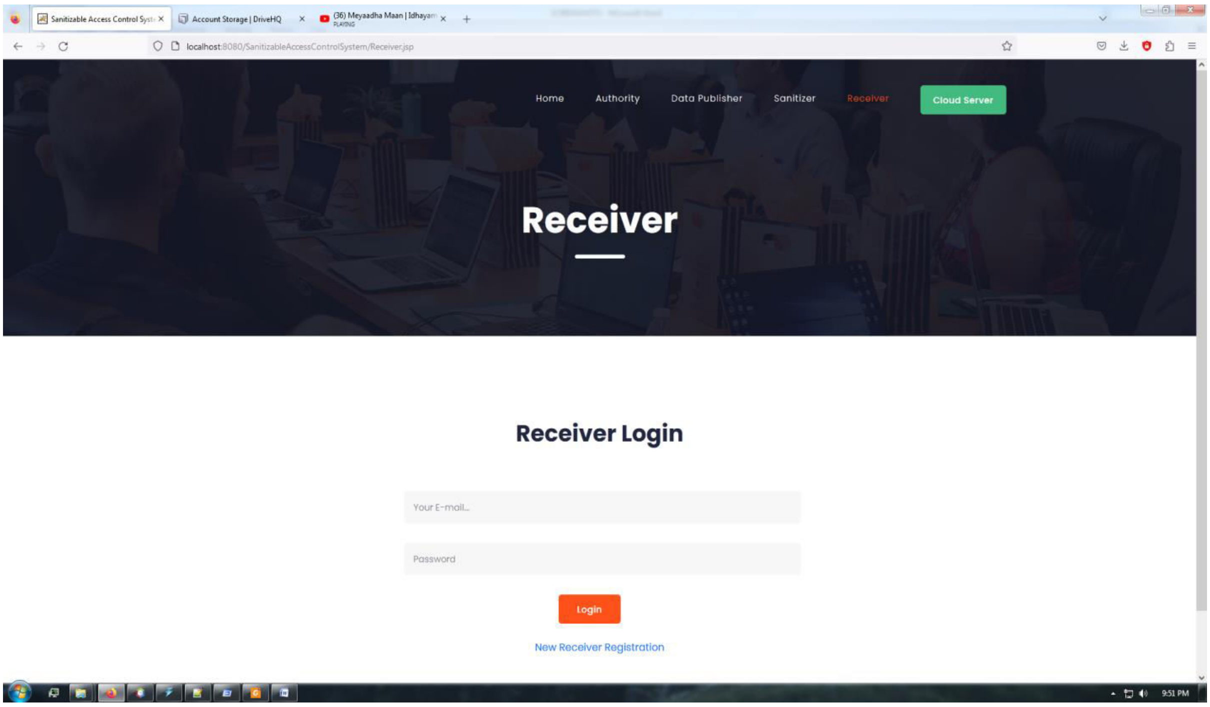

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) Meyaadha Maan | Idhayam
localhost:8080/SanitizableAccessControlSystem/Receiver.jsp
Home
Authority
Data Publisher
Sanitizer
Receiver
Cloud Server
Receiver
Receiver Login
Your E-mail..
Password
Login
New Receiver Registration
9:51 PM

Fig:2.4 Receiver login

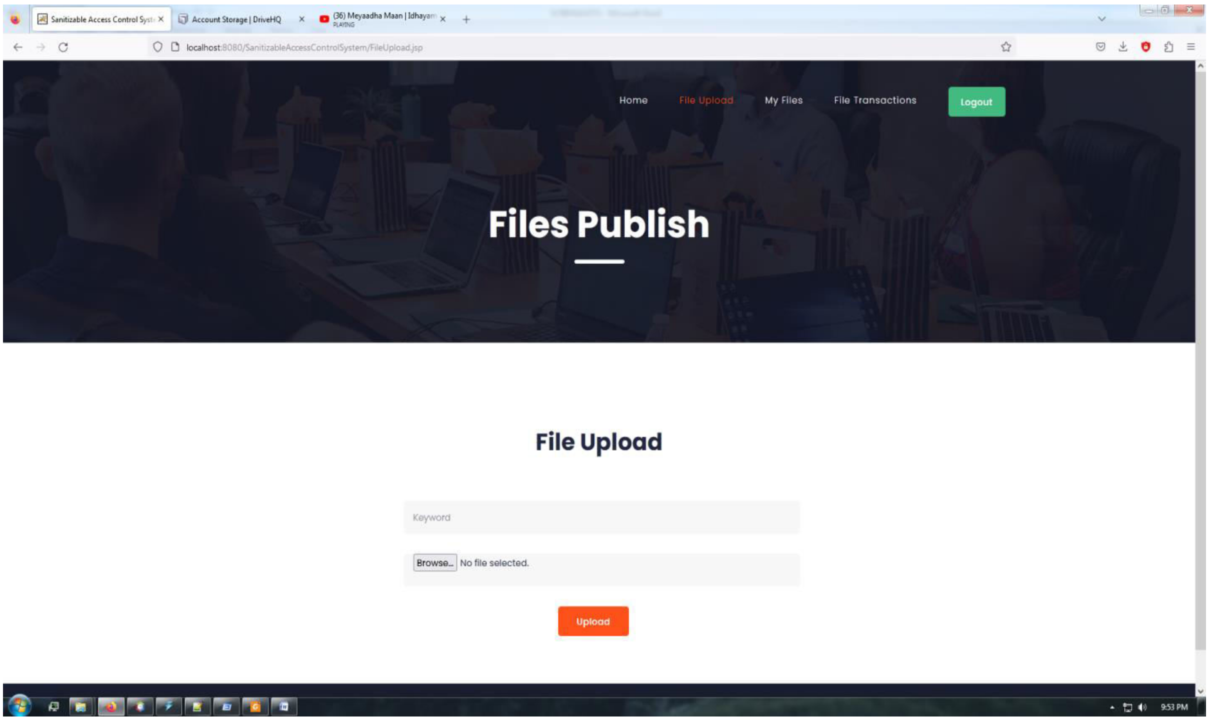
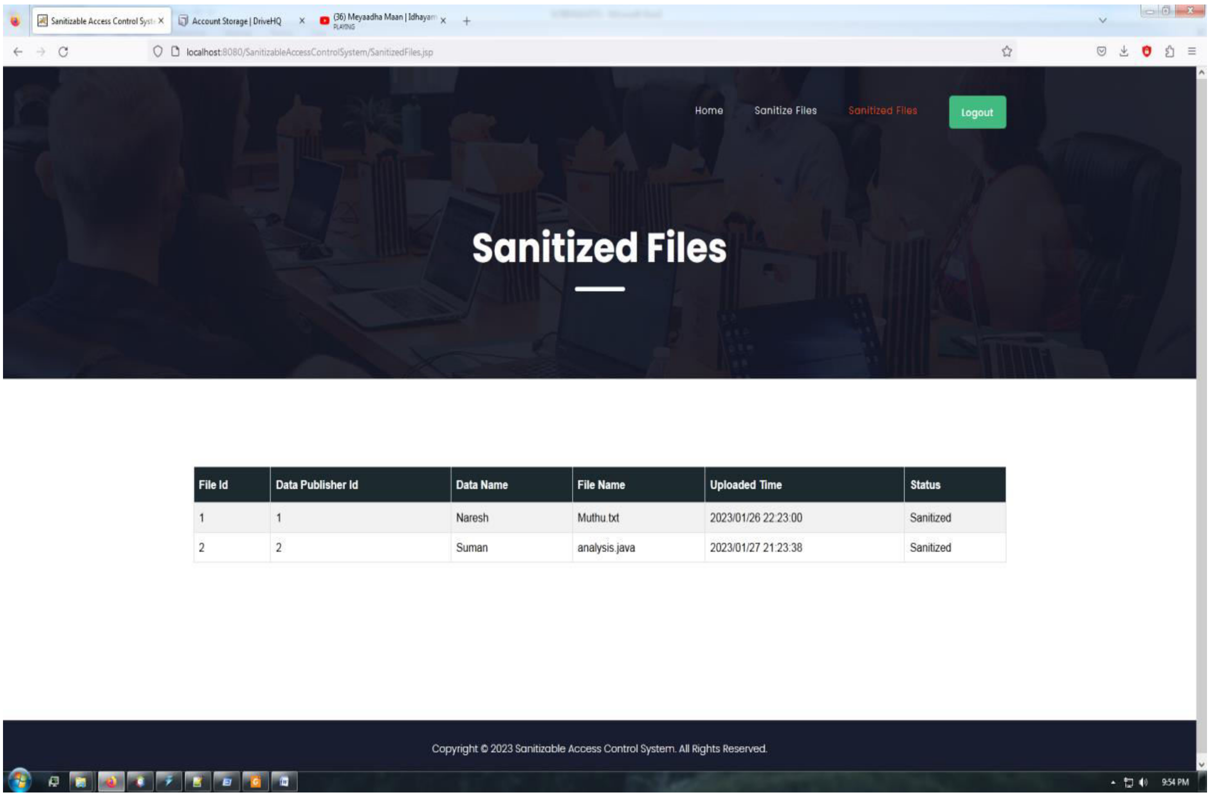

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) Meyaadha Maan | Idhayam
localhost:8080/SanitizableAccessControlSystem/FileUpload.jsp
Home
File Upload
My Files
File Transactions
Logout
Files Publish
File Upload
Keyword
Browse... No file selected.
Upload
9:53 PM

Fig:2.5: File Publish By data Publisher

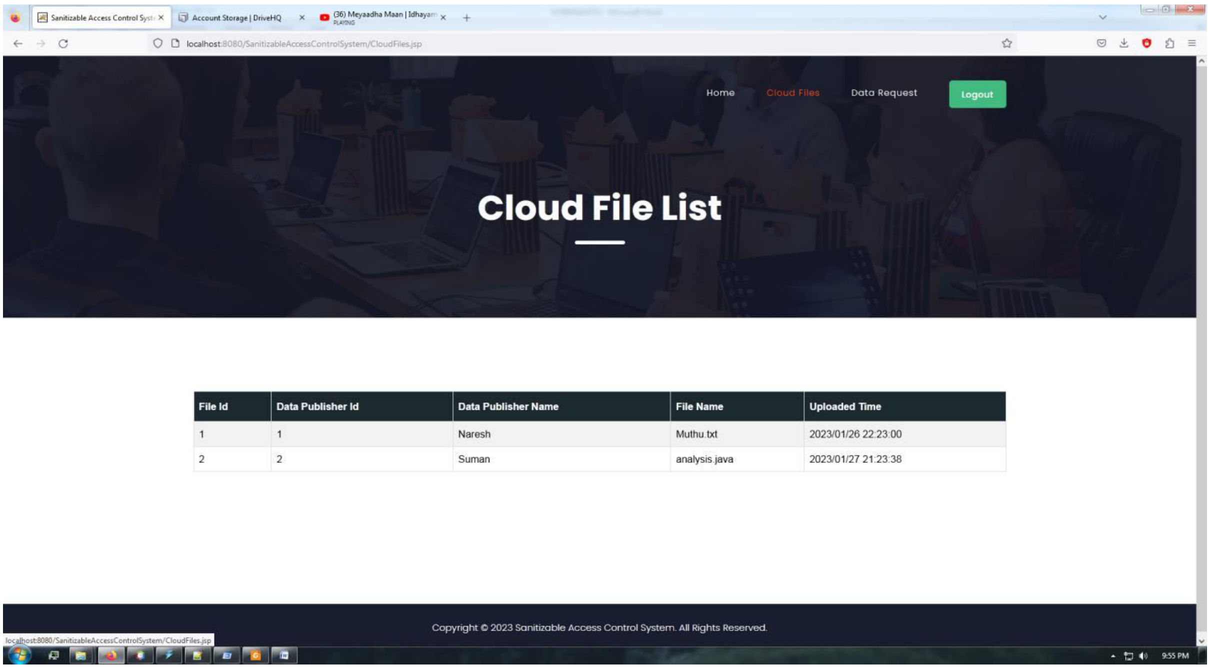

Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) Meyaadha Maan | Idhayam
localhost:8080/SanitizableAccessControlSystem/SanitizedFiles.jsp
Home
Sanitize Files
Sanitized Files
Logout
9:54 PM

Sanitized Files

File Id	Data Publisher Id	Data Name	File Name	Uploaded Time	Status
1	1	Naresh	Muthu.txt	2023/01/26 22:23:00	Sanitized
2	2	Suman	analysis.java	2023/01/27 21:23:38	Sanitized

Copyright © 2023 Sanitizable Access Control System. All Rights Reserved.

Fig :2.6 Sanitization of file


Sanitizable Access Control Syst
Account Storage | DriveHQ
(36) Meyaadha Maan | Idhayam
localhost:8080/SanitizableAccessControlSystem/CloudFiles.jsp
Home
Cloud Files
Data Request
Logout
9:55 PM

Cloud File List

File Id	Data Publisher Id	Data Publisher Name	File Name	Uploaded Time
1	1	Naresh	Muthu.txt	2023/01/26 22:23:00
2	2	Suman	analysis.java	2023/01/27 21:23:38

Copyright © 2023 Sanitizable Access Control System. All Rights Reserved.

Fig 2.7 List of files in cloud

VI. CONCLUSION AND FUTURE WORK

In conclusion, our study addresses the critical issue of secure cloud storage in the presence of malicious data publishers, a scenario previously overlooked in existing literature. By introducing this practical setting, where data publishers can construct data adhering to access control policies, yet the ciphertexts remain vulnerable to unauthorized decryption, we have developed a novel system and secure scheme to counteract such threats effectively. Our implementation and performance analysis further validate the feasibility and efficacy of our approach.

We anticipate that our pioneering work will catalyze future research endeavors in the domain of cloud storage security. By shedding light on this overlooked aspect, we aim to spur advancements that not only bolster the security of cloud storage systems but also enhance their practicality and reliability. Ultimately, we envision our contributions fostering greater confidence in adopting cloud storage solutions, as they offer enhanced protection against malicious actors and promote the integrity of sensitive data in cloud environments.

REFERENCES

[1] W. Susilo, P. Jiang, J. Lai, F. Guo, G. Yang and R. H. Deng, "Sanitizable Access Control System for Secure Cloud Storage against malicious data Publishers”
https://ieeexplore.ieee.org/document/9351678
[2] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,”
https://ieeexplore.ieee.org/document/4223236
[3] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, “Attribute based access control,”
https://ieeexplore.ieee.org/document/7042715
[4] Y. Wu, Z. Wei, and R. H. Deng, “Attribute-based access to scalable media in cloud-assisted content sharing networks”.
https://ieeexplore.ieee.org/document/6409463
[5] J. Hur, “Improving security and efficiency in attribute-based data sharing,”
https://ieeexplore.ieee.org/document/5740890

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