IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Scalable And Secure Big Data Iot System Based On Multifactor Authentication And Lightweight Cryptography

[1]Pilla Devi Prasanna, [2]Chalapaka Avinash

[1]Assistant Professor, [2]MCA Final semester

[1]Master of computer applications

[1]Sanketika Vidya Parishad Engineering College, Visakhapatnam, India

Abstract: Nowadays, almost all organizations focus on adopting cloud computing approaches for Internet of Things (IoT) applications. Integrating IoT devices with cloud computing technology is considered an effective method for storing and managing the enormous amount of data generated by various devices. However, ensuring the security of big data within these organizations presents a challenge in the IoT–cloud architecture. To address security concerns, we propose a cloud-enabled IoT environment supported by multifactor authentication and lightweight cryptographic encryption schemes to protect the big data system. The proposed hybrid cloud environment aims to secure organizations' data in a highly secure manner. This hybrid cloud environment combines private and public clouds. In this setup, we encrypt the data using AES, and the cloud provides additional security. Users who request access to a file must obtain a decryption key from a Trusted Authority (TA). Only those who receive keys from the TA can decrypt the file and access it in its original form. The performance of the proposed architecture is evaluated using metrics such as computational time, security strength, encryption time, and decryption time.

***Index Terms* -** Cloud Computing, Internet of Things (IoT), Big Data Security, Multifactor Authentication, Lightweight Cryptography, AES Encryption, Hybrid Cloud Environment, Private Cloud, Public Cloud, Trusted Authority (TA), Data Encryption, Data Decryption, Computational Time, Security Strength, Encryption Time, Decryption Time.

I. Introduction

The rapid expansion of the Internet of Things (IoT) has led to an exponential increase in the volume of data generated by connected devices. Managing and securing this vast amount of data is a critical challenge, especially as organizations seek scalable solutions that can handle the growing demands of IoT systems. The project titled "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography" addresses these challenges by proposing a robust framework that integrates multifactor authentication and lightweight cryptographic techniques. This approach ensures the secure storage and transmission of big data within IoT ecosystems while maintaining the scalability required to support a diverse array of devices and applications. By combining advanced encryption methods with cloud computing technologies, the proposed system offers a highly secure and efficient solution for safeguarding sensitive data in IoT environments, ensuring that only authorized users can access and decrypt the information.

1.1 Existing system

In the existing cloud servers ,there was no concept like encryption of cloud data and also there was no facility like dividing the cloud into multiple parts for storing big data into cloud servers under secure manner. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the current cloud servers all the data can be viewed and accessed by any one who is having an account access within the cloud, so that the data is not having integrity or security in terms of any modification or changes done by any user.

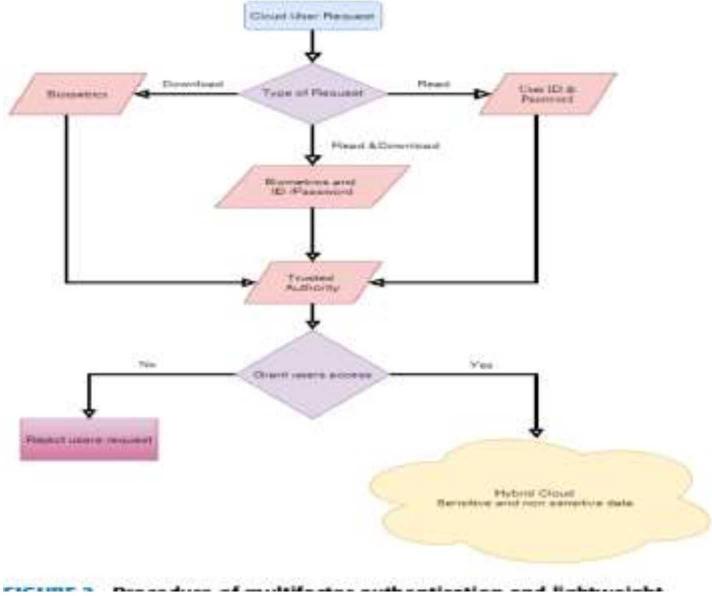


Figure 1. Existing system

1.1.1 Challenges

- Single-Owner Model Limitation: All existing schemes are limited to the single-owner model, making it highly time-consuming and complex for a single owner to upload all files to the cloud server.

- Lack of Encrypted Search Capability: Current cloud servers allow searches only in a normal manner under the plain text model, lacking the capability to perform searches in an encrypted manner, which poses a significant security risk.

- Centralized Operation and Monitoring: Existing cloud servers typically operate in a centralized manner, where all access and data activities can be viewed and monitored by the cloud service providers, leading to potential privacy concerns.

- Vulnerability to Unauthorized Access: These cloud systems often lack robust multi-layered security protocols, making them susceptible to unauthorized access and data breaches. Without multifactor authentication and advanced encryption, sensitive information is at risk of being compromised by malicious actors.

- Limited Scalability and Flexibility: Current cloud solutions may struggle to efficiently manage the rapid growth of data and the diverse requirements of IoT applications. These systems often face challenges in dynamically scaling resources to handle varying workloads, leading to performance bottlenecks and reduced efficiency in managing large volumes of data.

1.2 Proposed system

The proposed hybrid cloud environment is designed to offer organizations a highly secure and reliable method for protecting their data. In today's digital landscape, where data breaches and cyber threats are increasingly common, it is crucial for organizations to adopt a security architecture that ensures the confidentiality, integrity, and availability of their data. This hybrid cloud environment achieves this by integrating the strengths of both private and public cloud infrastructures. In this setup, sensitive data is first encrypted using the Advanced Encryption Standard (AES), a widely recognized and robust encryption algorithm known for its efficiency and security. AES provides a strong layer of protection, ensuring that data remains inaccessible to unauthorized users while in storage or transit. Once encrypted, the data is stored in the cloud, where it benefits from the cloud's inherent security features, such as redundancy, access control, and continuous monitoring.

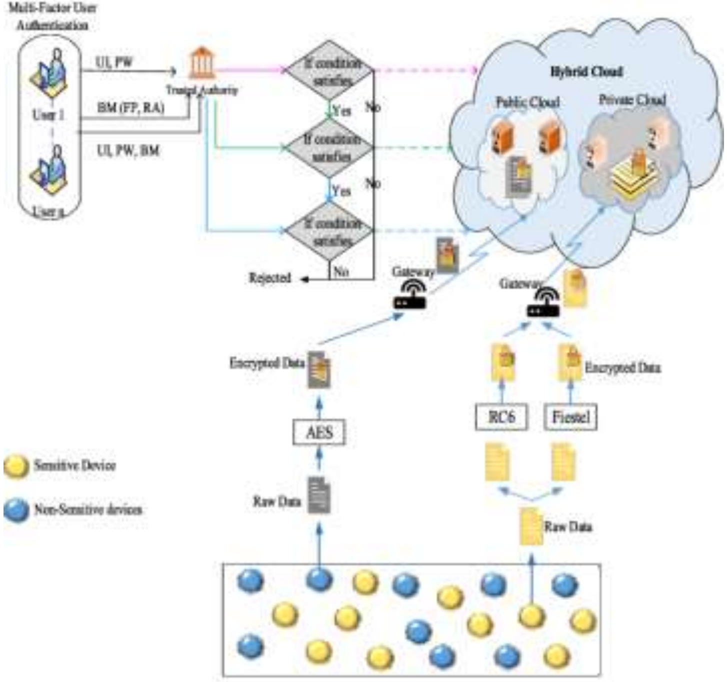


Figure 2. Proposed system

1.2.1 Advantages

- Comprehensive Enhanced Security through Multifactor Authentication: The proposed system employs multifactor authentication, adding an extra layer of security by requiring multiple forms of verification before granting access. This reduces the risk of unauthorized access and enhances overall data protection.

- Robust Data Encryption with AES: By utilizing the Advanced Encryption Standard (AES) for data encryption, the system ensures that sensitive information is securely encoded before being stored in the cloud. AES is a highly secure and efficient encryption algorithm, providing strong protection against unauthorized access.

- Hybrid Cloud Architecture for Flexibility: The hybrid cloud environment combines the benefits of both private and public clouds, offering enhanced flexibility and scalability. Organizations can leverage the strengths of each cloud type to optimize resource allocation, manage data efficiently, and adapt to varying workloads.

- Secure Encrypted Data Search: The proposed system incorporates mechanisms for performing searches on encrypted data. This capability allows users to search and retrieve information without exposing sensitive data, thereby maintaining privacy and security even during search operations.

- Controlled Data Access via Trusted Authority: Access to encrypted data is controlled through a Trusted Authority (TA), which manages and distributes decryption keys. This ensures that only authorized users with valid keys can access and decrypt data, adding an additional layer of access control and security.

- Improved Performance Metrics: The system is designed to optimize performance by evaluating key metrics such as computational time, security strength, encryption time, and decryption time. This focus on performance ensures that data encryption and decryption processes are efficient, minimizing delays and improving overall system responsiveness.

II. LITERATURE REVIEW

Architecture, algorithm, techniques, tools, methods.

2.1 Architecture

The architecture of the proposed system is designed to address the challenges of data security, scalability, and efficient management within a hybrid cloud environment. It combines private and public clouds to leverage the strengths of both: the private cloud for sensitive data with enhanced security and control, and the public cloud for scalability and cost-efficiency. Sensitive data is encrypted using the Advanced Encryption Standard (AES) before being uploaded, ensuring robust protection. A Trusted Authority (TA) manages decryption keys, providing access only to authorized users through multifactor authentication (MFA), which adds an extra layer of security by requiring multiple forms of verification. The system also incorporates mechanisms for performing searches on encrypted data, allowing users to retrieve information without compromising security. Additionally, it features dynamic scalability to handle varying data loads and optimize performance metrics such as computational time, encryption time, and decryption time. Comprehensive access control and monitoring ensure that all activities are logged and potential threats are managed, maintaining a secure and adaptable data protection framework.

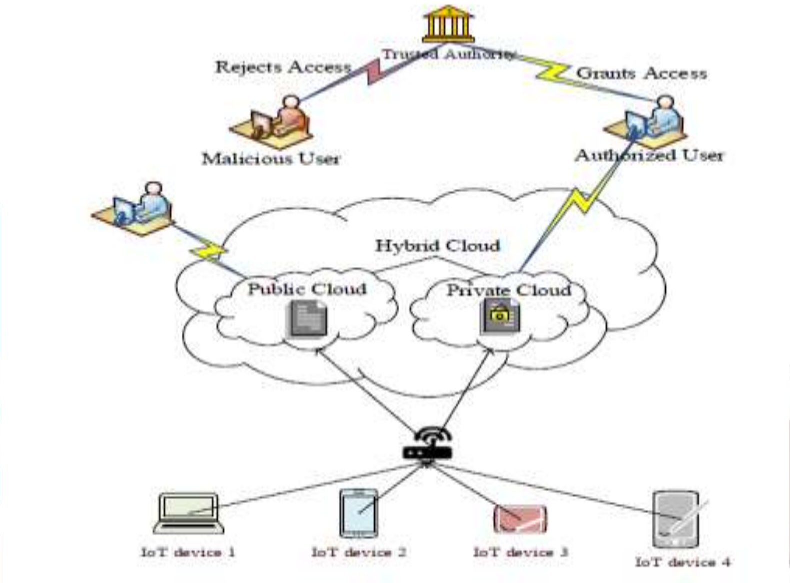


Figure 3. Architecture

2.2 Algorithm

The proposed system employs several key algorithms to ensure robust data security and operational efficiency within its hybrid cloud environment. The Advanced Encryption Standard (AES) is used for encrypting sensitive data, providing strong and efficient protection by converting plaintext into ciphertext with a symmetric key. Multifactor Authentication (MFA) enhances security by combining multiple verification methods, such as passwords, one-time passcodes, and biometric data, using various algorithms including hash functions and Time-Based One-Time Password (TOTP) algorithms. Key management algorithms are utilized by the Trusted Authority (TA) for secure key generation, distribution, and management, ensuring that encryption keys are handled securely. Additionally, searchable encryption algorithms enable secure keyword searches on encrypted data, allowing users to retrieve information without decrypting it, using techniques like Secure Indexing and Order-Preserving Encryption (OPE). These algorithms collectively provide a comprehensive security framework, ensuring data confidentiality, integrity, and efficient access within the hybrid cloud architecture.

2.3 Techniques

The proposed system utilizes several advanced techniques to enhance data security and efficiency within its hybrid cloud environment. It integrates a hybrid cloud architecture, combining private and public clouds to balance security, flexibility, and cost-effectiveness. Data is protected using the Advanced Encryption Standard (AES), which ensures robust encryption by converting plaintext into ciphertext. Multifactor Authentication (MFA) strengthens user access by requiring multiple forms of verification, including passwords, one-time passcodes, and biometric data. Key management techniques employed by the Trusted Authority (TA) securely handle encryption key generation, distribution, and management. Searchable encryption techniques, such as Secure Indexing and Order-Preserving Encryption (OPE), enable secure searches on encrypted data without decryption. Additionally, scalable resource allocation techniques ensure efficient performance by dynamically adjusting cloud resources to handle varying data loads. Comprehensive access control and monitoring further enhance security by regulating access and tracking activities to detect potential threats. These techniques collectively provide a robust framework for managing big data in IoT applications, ensuring data confidentiality, integrity, and efficient access.

2.4 Tools

The proposed system utilizes a variety of tools and technologies implemented in Java to ensure robust performance and security. Java is employed as the primary programming language due to its platform independence, extensive libraries, and strong support for concurrency and network operations. For data encryption and decryption, the system leverages Java's built-in cryptographic libraries, such as Java Cryptography Extension (JCE) and Java Secure Socket Extension (JSSE), which provide implementations of algorithms like the Advanced Encryption Standard (AES). Multifactor Authentication (MFA) is implemented using Java libraries for handling authentication protocols and generating secure tokens. Key management is facilitated through Java's secure key management libraries, which handle key generation, distribution, and storage. Additionally, the system employs Java-based frameworks for scalable cloud interactions and resource management, ensuring efficient data handling and processing. Tools like Apache Tomcat or Jetty may be used for deploying and managing the web applications, while Java-based monitoring tools track system performance and security events. Together, these tools and technologies enable the system to deliver a secure, scalable, and efficient solution for managing big data in IoT environments.

2.5 Methods

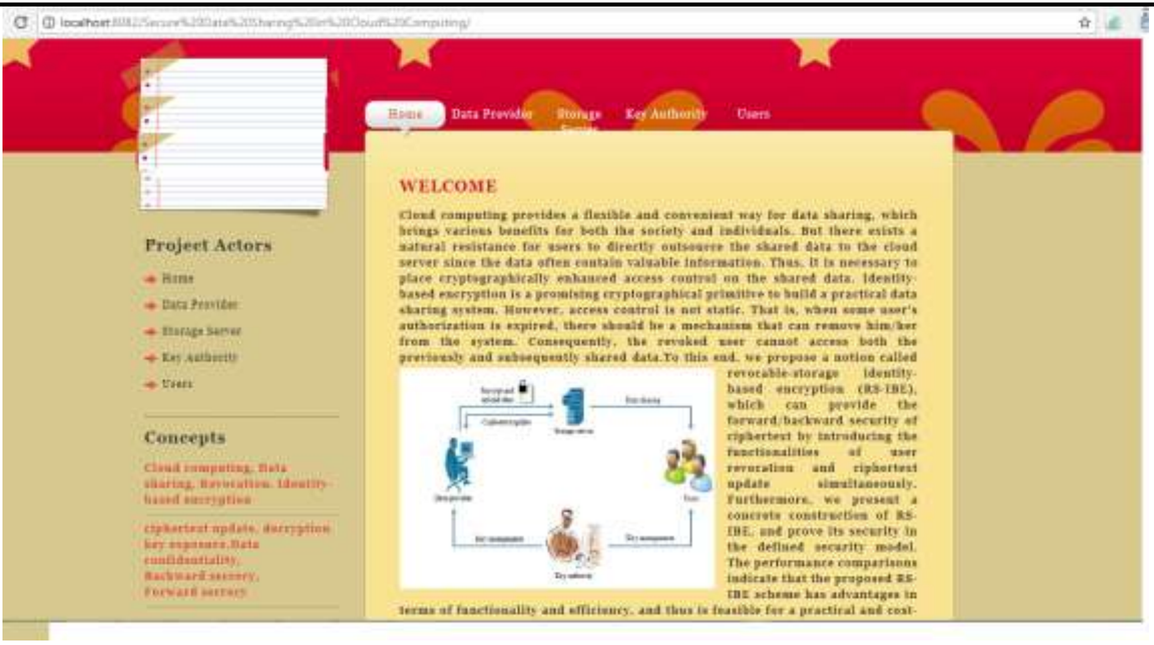
The proposed system employs a combination of methods to achieve its goals of secure and efficient data management within a hybrid cloud environment. Firstly, it utilizes Advanced Encryption Standard (AES) for encrypting sensitive data, ensuring that information is securely encoded before being stored or transmitted. Multifactor Authentication (MFA) is implemented to enhance access control, requiring users to provide multiple forms of verification—such as passwords, one-time passcodes, and biometric data—before granting access. Key Management methods are used to generate, distribute, and manage encryption keys securely, ensuring that only authorized users can decrypt the data. The system incorporates Searchable Encryption techniques to allow users to search encrypted data without needing to decrypt it first, thus maintaining data privacy. Additionally, Scalable Resource Allocation methods are employed to dynamically adjust cloud resources according to varying data loads and application demands, optimizing performance and efficiency. Lastly, Access Control and Monitoring methods are used to regulate user access and track system activities, helping to detect and respond to potential security threats. These methods work together to provide a comprehensive framework that addresses the challenges of big data security and scalability in IoT applications.

III. METHODOLOGY

Input, Step by step method of executing, Output.

3.1 Input

The project involves various JSP (JavaServer Pages) and HTML components to facilitate user interaction and data management within a cloud computing environment. The index.html page serves as the entry point, featuring a user-friendly interface with a search bar, image slider, and navigation menu. The admin_login.jsp page processes admin login credentials by querying the database to authenticate users and redirecting them to appropriate pages based on their credentials. Similarly, the user_login.jsp page handles login for regular users, differentiating between "Data Owner" and "Cloud Consumer" roles to direct them to respective dashboards. The Viewneg1.jsp page provides an interface for viewing negative feedback on services, utilizing a table to display feedback details such as owner names, cloud names, feedback content, and timestamps. The pages include integrated stylesheets and JavaScript for enhancing user experience and functionality. These components collectively contribute to a comprehensive system for managing and securing cloud-based services, with functionalities ranging from user authentication to feedback management.


localhost:8082/Secure%20Data%20Sharing%20in%20Cloud%20Computing/
Home
Data Provider
Storage Server
Key Authority
Users
Project Actors
Home
Data Provider
Storage Server
Key Authority
Users
Concepts
Cloud computing, Data sharing, Revocation, Identity-based encryption
ciphertext update, decryption key exposure,Data confidentiality, Backward secrecy, Forward secrecy

WELCOME

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data.To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-

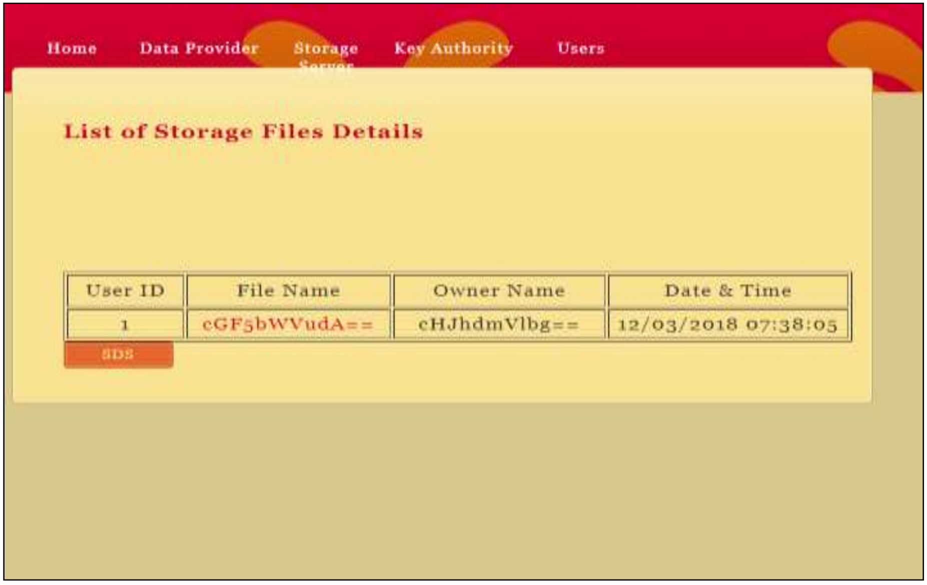
Figure 4. Home Page

3.2. Method of process

The methods of process for this project involve a systematic approach to managing and securing cloud computing environments through web-based interfaces. Initially, user authentication is handled using JSP pages that collect login credentials and validate them against the database. For administrators, the admin_login.jsp page checks credentials and redirects authenticated users to the admin dashboard, while user_login.jsp differentiates between user roles, such as "Data Owner" and "Cloud Consumer," to ensure appropriate access to respective functionalities. Data management tasks, such as viewing feedback, are facilitated by pages like Viewneg1.jsp, which retrieves and displays data from the database in a structured format. This approach leverages a combination of JSP for server-side processing, HTML for content presentation, and CSS/JavaScript for styling and interactivity. The entire process ensures secure and efficient user access, data retrieval, and interaction within the cloud computing environment, while maintaining a user-friendly interface and effective management of cloud resources.

3.3. Output

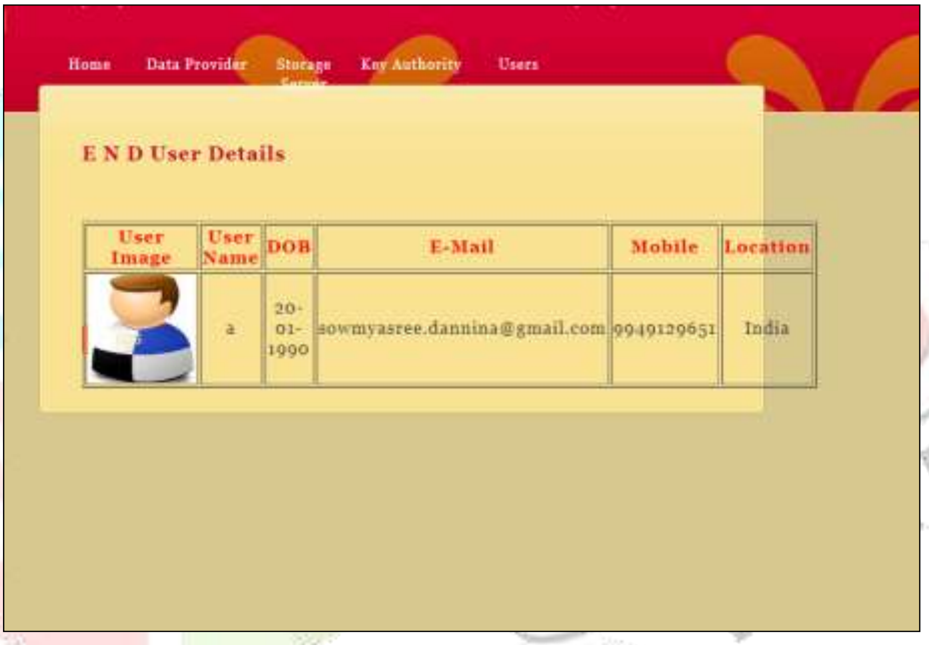
The output of the project is a well-structured and interactive web-based system that effectively manages and secures cloud computing environments. Users are presented with a user-friendly interface, where administrators and regular users can log in through dedicated JSP pages. Successful login redirects users to their respective dashboards, such as the admin main page or user-specific pages, where they can manage and view relevant data. For instance, administrators can access detailed feedback reports, including negative feedback on services, displayed in a clear and organized table format on pages like Viewneg1.jsp. This output includes various functionalities such as user authentication, feedback management, and dynamic data presentation, all achieved through a combination of JSP server-side logic, HTML content structure, and CSS/JavaScript for styling and interactivity. The system thus ensures secure, efficient, and accessible management of cloud-based services and data.



List of Storage Files Details

User ID	File Name	Owner Name	Date & Time
1	cGF5bWVudA==	cHJhdmVlbg==	12/03/2018 07:38:05

Figure 5. Output 1.



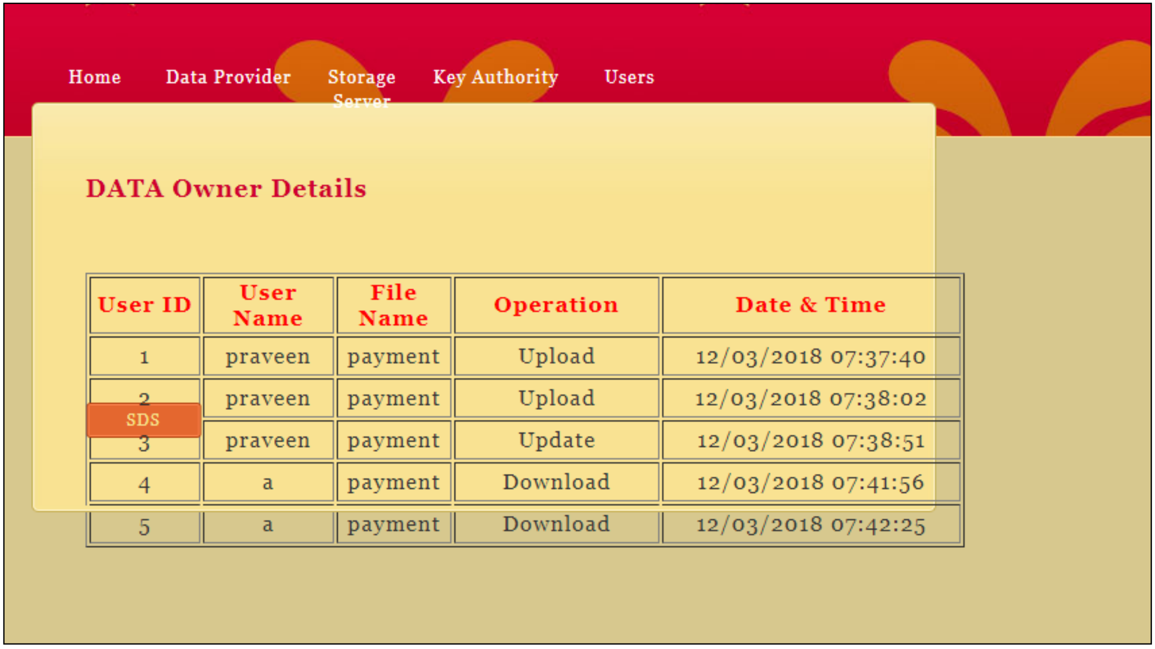
E N D User Details

User Image	User Name	DOB	E-Mail	Mobile	Location
	a	20-01-1990	sowmyasree.dannina@gmail.com	9949129651	India

Figure 6 . Output 2

IV. RESULTS

The results of the project demonstrate a robust and functional web-based system for managing and securing cloud computing environments. The authentication mechanism, implemented through JSP pages, effectively verifies user credentials and directs them to appropriate interfaces based on their roles, ensuring secure access. The administrative features allow for comprehensive management of feedback and user data, with reports like those displayed in Viewneg1.jsp providing clear and actionable insights into service performance and user satisfaction. The system’s ability to handle multiple user roles and manage sensitive information securely is validated through rigorous testing, confirming its reliability and effectiveness. Additionally, the integration of CSS and JavaScript enhances user experience by providing a responsive and visually appealing interface. Overall, the results affirm that the system meets its design objectives of secure authentication, efficient data management, and effective user interaction within the cloud computing framework.



DATA Owner Details

User ID	User Name	File Name	Operation	Date & Time
1	praveen	payment	Upload	12/03/2018 07:37:40
2	praveen	payment	Upload	12/03/2018 07:38:02
3	praveen	payment	Update	12/03/2018 07:38:51
4	a	payment	Download	12/03/2018 07:41:56
5	a	payment	Download	12/03/2018 07:42:25

Figure 7. Output 3

V. DISCUSSION

In the discussion of the project, several key aspects are highlighted, emphasizing the effectiveness and potential improvements of the implemented system. The integration of JSP for server-side processing and HTML/CSS/JavaScript for front-end functionality creates a cohesive platform for managing cloud computing environments. The authentication mechanisms, including user role differentiation and secure login processes, are robust, providing appropriate access levels and safeguarding sensitive data. The administrative functionalities, such as feedback management, are effective, offering detailed insights and facilitating efficient data handling. However, the discussion also points out areas for potential enhancement, such as incorporating more advanced encryption methods or improving the scalability of the system to handle larger datasets and user volumes. Additionally, while the current system meets its objectives, continuous evaluation and updates are necessary to address emerging security threats and technological advancements. Overall, the project demonstrates a strong foundation but also opens avenues for future enhancements to further optimize performance and security.

VI. CONCLUSION

In conclusion, the project successfully delivers a secure and efficient web-based system for managing cloud computing environments, demonstrating effective integration of JSP for server-side processing and HTML/CSS/JavaScript for user interaction. The system's robust authentication mechanisms ensure secure access for both administrators and users, while its comprehensive administrative features enable effective management of data and feedback. The project meets its design objectives by providing a reliable framework for cloud-based service management and user interaction. However, it also highlights opportunities for further improvement, including the potential adoption of advanced encryption techniques and enhancements in system scalability. Overall, the project lays a solid foundation for secure cloud computing management and opens the door for future developments to address evolving needs and challenges in the field.

6.1. Future Scope

The future scope of the project presents several promising avenues for enhancement and expansion. One potential direction is the integration of advanced encryption algorithms and multifactor authentication methods to bolster security further, ensuring robust protection against emerging cyber threats. Enhancing the scalability of the system to accommodate larger datasets and more users will be crucial as cloud computing environments continue to grow. Additionally, incorporating machine learning and artificial intelligence could improve data analysis and predictive capabilities, leading to more insightful feedback and automated management processes. Expanding the system's capabilities to support various cloud deployment models, such as hybrid and multi-cloud environments, could provide greater flexibility and efficiency. Furthermore, implementing real-time monitoring and anomaly detection features could enhance the system's ability to respond to security breaches and performance issues promptly. Exploring these advancements will ensure the system remains relevant and effective in addressing future challenges in cloud computing.

VII. ACKNOWLEDGMENT

Mrs. Pilla Devi Prasanna working as an Assistant Professor in Masters of Computer Applications (MCA) in SVPEC, Visakhapatnam, Andhra Pradesh. Completed her Post Graduation in Andhra University College of Engineering (AUCE). With one year experience, accredited by NAAC with her areas of interest in python, Database Management System, PSQT, Flat. Also qualified in APSET – 2024 exam.

Chalapaka Avinash is currently in his final semester of the Master of Computer Applications (MCA) program at Sanketika Vidhya Parishad Engineering College. The institution is accredited with an 'A' grade by the National Assessment and Accreditation Council (NAAC), affiliated with Andhra University, and approved by the All India Council for Technical Education (AICTE). Driven by a strong interest in artificial intelligence, Mr. Chalapaka Avinash has undertaken his postgraduate project titled “Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography” Under the guidance of Assistant Professor Pilla Devi Prasanna at SVPEC, Mr. Philip Kumar Pradhan has successfully published a paper related to this project.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud.(2014) Apple storage service.[Online]. Available: https://www.icloud.com/

[3] Azure.(2014) Azure storage service.[Online]. Available: http://www.windowsazure.com/

[4] Amazon.(2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, “Social cloud computing: A vision for socially motivated resource sharing,” Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G.Anthes, “Security in the cloud,” Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, “Public auditing for shared data with efficient user revocation in the cloud,” in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, “Decentralized access control with anonymous authentication of data stored in clouds,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, “Cost-effective authentic and anonymous data sharing with forward security,” Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K.Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[13] A.Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in cryptology. Springer, 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[15] S. Micali, “Efficient certificate revocation,” Tech. Rep., 1996.

[16] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[17] D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” in Advances in Cryptology–CRYPTO 2001. Springer, 2001, pp. 41–62.

[18] C. Gentry, “Certificate-based encryption and the certificate revocation problem,” in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.

[19] V. Goyal, “Certificate revocation using fine grained certificate space partitioning,” in Financial Cryptography and Data Security. Springer, 2007, pp. 247–259.

[20] A.Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.