International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Integrated Cloud Security Framework for Confidentiality Integrity Availability with Multi Access Control

Himaja A. V[1], Guljar. Shailk[2], Tejaswini D.V[3], Jagan Raja. V[4]

[1,2,3]Department of CSEVeltech University), Chennai, India.
[4]Assistant Professor, Department of CSEVeltech University Chennai, India

Abstract

This research seeks to design and deploy a robust data protection system based on cloud computing enhanced with multiple access creation methods, aimed at providing privacy, integrity and information a the importance of existing in an era of digital land domination has improved, protecting data Most importantly, this system addresses the needs of scope answer. This means that we have created a system that keeps only data confidential It is accessible to authorized users, ensures data integrity and maintains it immutable Integrity, and guarantees that the services are always accessible and widely available. We built this system using MongoDB, which is a powerful and flexible storage platform Safe data in the cloud. This process ensures that only the right people Allows access to critical information using role-based user interfaces. This is the reason Everyone has the right access they need for their job, nothing more and Nothing less than that. The system also prioritizes availability through redundancy and. Failure mechanisms, in order to ensure smooth service delivery. Multi-access control The capability enables access to custom content based on pre-defined settings and users Opportunities .

IndexTerms: Confidentiality, Integrity, Availability, Cloud Framework, Multi Access control, User Authentication.

I. INTRODUCTION

In today's digital age, the adoption of cloud computing has changed course Organizations manage and store their data. Cloud technology offers scalability, flexibility and lower costs, making it desirable for businesses of all sizes. However, with the advantages of cloud computing comes great challenges, especially in terms of data security, integrity and availabil- ity.Taking advantage of the state-of-the-art Technologies and processes, the framework aims to provide comprehensive and dynamic solutions designed to exceed traditional security systems landscape of cyber threats.By adding caution to cloud computing power and advanced safety systems, this research aims to empower A foundation for securing sensitive informa- tion, enabling organizations to navigate the digital landscape with confidence.The introduction to this work emphasizes The need for a robust and holistic approach to cloud security. Customary protection Typically, strategies are insufficient in the distributed dynamic nature of cloud computing, where data can traverse multiple networks and be accessed from different locations equipment and facilities.Integration of multiple secu- rity systems a An integrated system, enables organizations to establish strong defenses against developments cyber threats as well as

ensuring compliance with legal requirements. It goes beyond traditional service delivery by offering features on the platform Food donations, trash cleanup and drainage systems, each monitored Selected organizations NGOs and municipalities. Using MongoDB for complex data Storage and recovery, our business prioritizes security, ensures privacy and guarantees unlimited user access with authentication. Focusing on the story Multi-access control, we are revolutionizing how critical services are managed and. accessible, resulting in an effective and safe community support system .

II. LITERATURE REVIEW

Zissis, D., Lekkas, D. (2012). Addressing cloud computing security issues. It provides a detailed analysis of the threats and vulnerabilities in cloud environments and proposes solutions to mitigate these issues. This literature review focuses on the main contributions of the paper, focusing on research on the privacy, integrity, availability, and security measures proposed. Encryption has been emphasized as the primary means of protecting data privacy. The paper looks at various approaches to encryption and the importance of key management prac- tices.Threats such as corrupted data, malicious changes and unauthorized changes are analyzed. The paper discusses how these threats can undermine the reliability and trustworthiness of data.

Yu, S., Wang, C., Ren, K., Lou, W. (2010) The paper begins with the main challenges associated with data processing in cloud computing . This approach addresses the fundamental challenges of data management and provides robust solutions for securing sensitive data in a cloud environment. The eval- uation results demonstrate the performance of the framework, making it a valuable reference for researchers and practitioners working on cloud security and access control techniques .

Ren, K., Wang, C., Wang, Q. (2012) The authors highlight several critical issues that need to be addressed to ensure the safe deployment and use of public cloud services. The main challenge is data security and privacy, as sensitive user information is stored on remote servers hosted by third-party cloud providers. Ensuring data confidentiality and integrity through strong encryption techniques and access control mea- sures is essential to preventing unauthorized access .Another important issue is the reliability of the cloud infrastructure. Users should rely on a cloud provider's assurance of the security and reliability of their services, with confidence that the providers have implemented appropriate security measures and their practices and security policies if stated around This trust is important because users cannot see the underlying and controlled infrastructure used to operate.

The paper also addresses the challenge of secure data sharing and processing. As more organizations use cloud services for collaboration, ensuring that data remains secure as it is shared across multiple users and applications becomes paramount They drive Device hear that secure mass computing and uniform encryption are discussed as potential solutions for secure data processing without privacy.

III. METHODOLOGY

A. General Architecture

In fig 1 shows a cloud infrastructure supports a Node.js application that connects to a MongoDB database. Security layers ensure integrity, . Encryption, access, and manage- ment. api gates and other external services Together they have increased performance. This model emphasizes privacy, integrity, availability, and multi-channel access, and aligns with goals .

B. Use Case Diagram

In fig 2 shows that types of actions and interactions between user and system . The users are the cloud

service user, the security auditor, and the administrator. Donate food,manage garbage address water leakage,etc Safety measures Food do- nation records,Coordinate garbage collection, prepare leak re- ports, and maintain safety operations and permits. This picture gives a high-level idea of how different it is Organizations interact with the system to achieve specific roles and functions.

C. Activity Diagram

In fig 3 shows that there is a sequence of activities and actions in the system. User Requests Service, NGO Regists Donations,City and other activities Deal with leaks and sim- ulate safety controls accordingly actions and decision points. Arrows indicate control flow between actions, . There are iter- ations and branches for decision making. Swimming channels can represent different actors or parts of the system involved in different activities, . Ensuring clarity in responsibility and communication. Functional diagrams help understand business flows, identify potential bottlenecks and optimize them settingsin the system design.

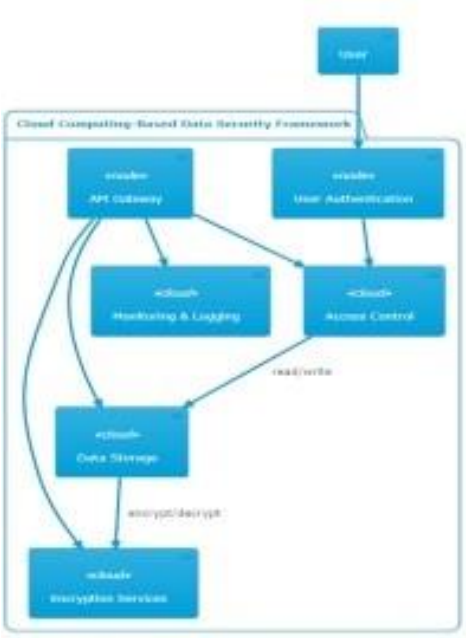

Fig. 1. Architecture Diagram for cloud computing and data security frame-work

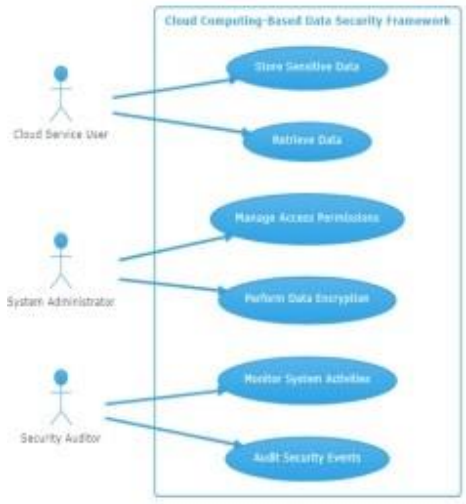

Fig. 2. Use case diagram for cloud computing and data security framewor

Fig. 3. Activity diagram for cloud computing and data security framework

IV. ALGORITHM AND PSEUDO CODE

A. Algorithm for Food donation service

- Receive requests indicating that the user or organization.
- Determine if the request is for a food donation service.
- If the request is from a food donation agency .
- verify the credentials of the NGO .
- If NGO credentials are valid: Accept food donations.

B. Algorithm for Garbage Cleaning Service

- Receive waste cleanup requests from the user or organi-zation.
- Ensure that the request is for a garbage disposal opera-tion.
- Ensure garbage washing service is available at the re-quested location.
- Collect waste from designated areas .
- Inform the user or organization that the waste stream iscomplete .

C. Algorithm for Water Leakage Service

- Obtain leak reports from the user or organization.
- Verifying the report to confirm a leak problem.
- Take immediate steps to stop leaks and prevent furtherdamage.
- Make corrective action based on the findings of theinspection and the nature of the issue.

D. PseudoCode

This pseudo code describes the basic functionality required for an integrated cloud security system, emphasizing user authentication, data encryption, access control, integrity check- ing, monitoring, incident response, continuing update, and user functionality Each functionality is designed to consume cloud protection of specific aspects of the environment .

V. HARDWARE REQUIREMENTS

- Processor : Intel i5 10th Generation
- RAM : 8GB
- ROM : 128GB
- Input Device : Keyboard, Mouse

A. Standards and Policies

VISUAL STUDIO:

VS Code is an open-source, lightweight code editor developed by Microsoft that supports a wide range of programming languages and frameworks. It provides features such as code completion, debugging, version control integration, and an extensive ecosystem of extensions for additional functionality . Many organizations using VS Code follow a Secure Development Lifecycle framework that incorporates security practices throughout the software devel- opment process. This includes threat modeling, code reviews for security vulnerabilities, security testing (such as static code analysis and penetration testing), and security training for developers .

Standard Used: ISO/IEC 27001

NODE.JS:

Node.js is a powerful runtime environment that allows developers to build server side applications using JavaScript. It follows a modular architecture and leverages an event-driven, non-blocking I/O model, making it ideal for developing scalable and high-performance applications.When developing Node.js applications, developers often adhere to industry standards and best practices to ensure security, reliability, and maintainability. One such standard which provides a framework for establishing, implementing, maintaining, and continually improving an ISMS.

Standard Used: ISO/IEC 27001

VI. MODULE DESCRIPTION

A. Authentication Integration

Design Authentication Protocols : Get a company Authen- tication protocols, a multifactor in it Authentication, to ensure that user identities control access Cloud-based systems.

Integrate Authentication into Framework : The equip- ment to be used Within the system are loyalty programs, to ensure simple user authentication during login and login The efforts they make.

Conduct Testing and Validation : Conduct a thorough test to validate encryption and authentication methods their efforts, ensuring that data remains secure and. Access only by authorized user .

B. Multiple Access Protection Layers

Define access points: Establish access points roles, permis- sions, and user profiles, define the specifics actions and data user groups can have.

Implemented Role-Based Permissions: Integrate Role- Based Access controls to ensure that only users have access Materials and capabilities necessary for their role in it system

Adaptive authentication implementation: its evolution Adaptive au thentication techniques use such Dynamically change the security level based on user's behavior, enhancing security against evolving threats .

Add session management: Use sessions Management con- trols for managing user sessions, including. timeouts, to- ken authentication, and secure session management, . further strengthening access security .

C. Security Analytics And Threat Detection

Select Analytical Tools : Identify and integrate security analytical tools capable of monitoring system operations, . net-work traffic, and user behavior to determine capacity Security threats.

Define anomaly detection criteria: Establish criteria for anomaly detection of normality Behavioral measures to detect abnormalities or Prejudiced actions.

Configure an automatic alert system: Use an automatic System alerts to notify operators in real time when Possible security risks or discrepancies are identified.

Conduct testing and optimization regularly: Regularly Analyze the effectiveness of security audits and threats Eval- uation methods and optimization criteria algorithms to en- hance the framework's ability to recognize and Respondingto Changing Cyber Threats .

VII. IMPLEMENTATION

A. Input Design

In fig 4 shows that the control strategy hit their target facil- itating effective communication and ease of use Transactions of the Forum. The submission button is conveniently placed When placed in each form, users can see the final look invests effortlessly. confirmation mode or messages Acknowledge and clarify successful submissions Guidelines for next steps .

B. Output Design

In fig 5 shows that in order to ensure the efficiency of the onboard users data security and accessibility. The firstpart takes over Personal information, including the user's full name and email address address, and contact number. This information is important for accounting integrity and communication purposes. next, Users are asked to create a unique combination of username and password. Users inthe next section indicate their role or relationship with the NGO (non-governmental organization) or municipality.To To enhance security and prevent unauthorized access, multifactor authentication (MFA) option is proposed, which allows Users link their accounts to a mobile number or email Another step of log-in authentication.

Fig. 4. Login page for access management

Fig. 5. Registration page for access management

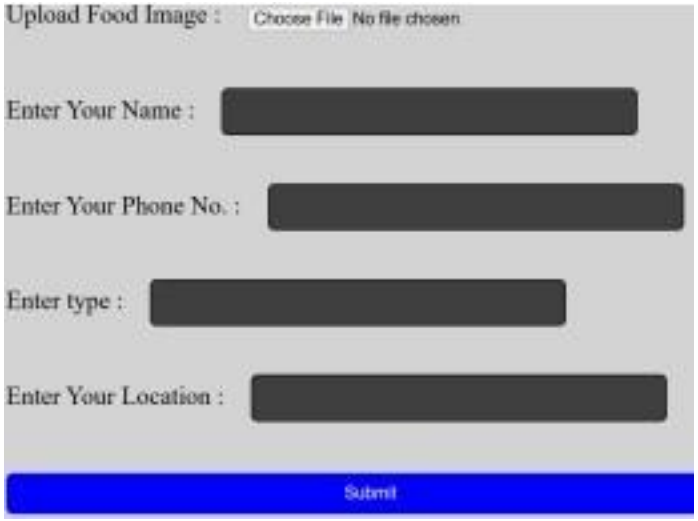

Fig. 6. Requesting for food donation

In fig 6 shows that the stakeholders in this aspect are at the core of the platform NGOs, are empowered to initiate and maintain donation campaigns and transparency.Users are welcomed when they enter the food donation department A user-friendly interface that guides them through the donation process. The stage is covered It provides users with optionsto specify the type of donation they wish to make, e.g. as a picture of the food , the user's personal details , location and submit the re quest.This versatility ensures that providers can help match them preferences and capabilities.Throughout the contribution process, the platform maintains high standards of security and data integrity through the use of the integrated cloud A security policy and MongoDB database to protect sensitive information and. Be sure to maintain confidentiality. Users can rest assured that their donation information is safe and handled with the utmost care.

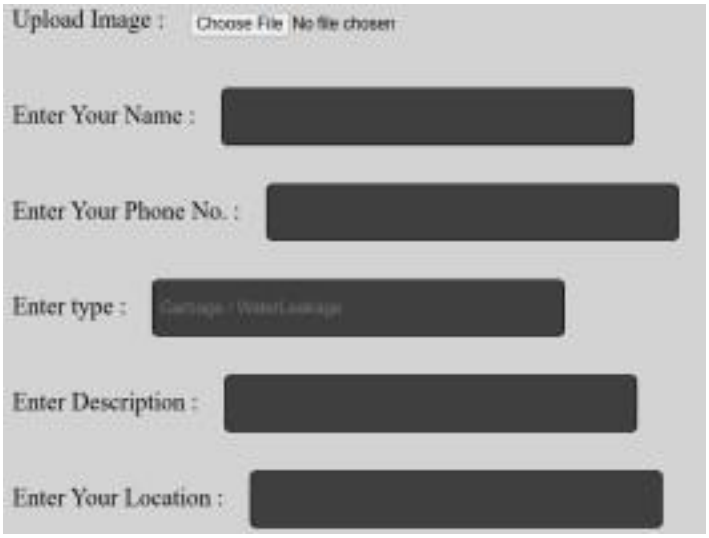

Fig. 7. Requesting for household

In fig 7 shows that the equivalent space is an intermediate solution for To access and participate in necessary services to keep residents clean, safe, and well cared for The Continuous Life. Concerns about leaks, residents can use A forum for quick reporting of events. The intuitive interface allows users to present it It provides detailed information on location, leaks and severity and facilitates rapid targeted response. The platform facilitates communication between community members and the municipality, in order to effectively monitor reported issues and provide updates on progress on solutions. Taking advantage of the platform power, the city can prioritize and address leak issues, a Timely reduction of water wastage and promotion of responsible water use in the community.

In fig 8 illustrates this process for sending feed requests to users donations, waste management, and leak information, to ensure a quick and effective response by designated organiza- tions, whether NGOs or municipalities.The The user request acknowledgment page is designed for user friendliness and functionality mind. It provides users with clear and intuitive investment areas and options a. type of request they wish to

Fig. 8. Page for accepting user's request

make.Users can choose from predefined requests Like food do- nations, garbage collection, or leak reporting, streamlining A request forwarding system ensures that requests are forwarded to the appropriate departments.Within each request category, users are prompted to provide a specific Information about their request. For food donation requests . and snowflakes Management requests, users can describe the problem, provide location information, and upload Appropriate images with

contact information .

Run the application in a production environment, or on a cloud platform Servers on site. Configure monitoring tools to monitor application performance, . resource usage, and real-time user interactions.Test the application thoroughly for errors, responsiveness, and performance. Perform unit testing of individual components and combination testing of the whole application flow.space.Conduct system testing to evaluate ap- plication behavior Overall, it also includes connections to external systems or databases.

VIII. CONCLUSION

In conclusion, the implementation of cloud computing- based data security The system with Multiple Access Pro- tection marks a significant step forward in tifying privacy, integrity and availability of sensitive information The digital landscape. By incorporating advanced encryption and authen- tication mechanisms, the system lays a solid foundation to protect data on Relax and cut. Combining access to multiple layers of security ensures that Only authorized users with the appropriate privileges can access sensitive information, provid- ing a secure and controlled environment. Also the beginning of safety Analysis and threat identification not only enhance proactive system defenses against emerging cyber threats but also enabling rapid response and mitigation

The project focused on enhancing security measures in big data systems Cloud computing is increasingly important and there are potential benefits across platforms For organizations operating in today's data-driven landscape. The use of ma- terials a Comprehensive security systems including polished access, Strong data encryption, multi-factor authentication, au- tomated compliance management, scalable architecture, highly managed security, and data integrity research, the proposed system addresses and improves important safety challenges the security level of all big data applications.All of these factors result together Cost savings, improved operational efficiency, and a more responsive and flexible system addressing emerg- ing security challenges.

IX. FUTURE ENHANCEMENT

There are many improvements that can be implemented in the future To make the given web platform more efficient and effective again Through services such as feeding, garbage cleaning and drainage management specific roles for NGOs and municipalities.Possible improvements could be Integration of machine learning algorithms and data analytics into the framework. Aging, compiled from user interactions, service requests, and comments, the product To predict service de- mand, learning models can be developed to optimize resource utilization participation and improve decision-making process. For example, the system can Use historical data to predict periods of peak food donation requests or identify trends Prioritize repair efforts in reporting leaks. This is a data driven approach It will not only enhance the overall user experience but also improve operational efficiency and service efficiency. Further future development could focus on expanding the range of services offered on the platform. While the current system provides essential services such as. There may be opportunities to incorporate additional services that address the needs of the broader community, including food supply, waste reduction, and drainage management. For example, en- vironmental sustainability, risk management, or. Public health initiatives can be incorporated into the platform to provide comprehensive and impactful solutions for communities. It would need to be expanded Collaboration with relevant stake- holders including government agencies, not-for-profit sectors

organizations, and community groups, to identify and prioritizenew service offerings that align with the platform's mission and objectives.

REFERENCES

1. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro and T. F. Pena, (2023) Security by Design for Big Data Frameworks Over Cloud Computing, in IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3676-3693 .
2. A. Balcao Filho, N. Ruiz, F. d. F. Rosa, R. Bonacin and M. Jino., (2023) Applying a Consumer-Centric Framework for Trust Assessment of Cloud Computing Service Providers, in IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 95- 107.
3. Djemame, K., Armstrong, D., Guitart, J., Macias, M. A risk assessment framework for cloud computing. IEEE Transactions on Cloud Comput- ing,2011, 1(1), 53-65 .
4. H. Ma, R. Zhang, S. Sun, Z. Song and G. Tan, (2023) Server-Aided Fine- Grained Access Control Mechanism with Robust Revocation in Cloud Computing, in IEEE Transactions on Services Computing, vol. 15, no.1, pp. 164-173.
5. Ren, K., Wang, C., Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing,2012 16(1), 69-73
6. Sun, D., Chang, G., Sun, L., Wang, X. Surveying and analyzing security, privacy, and trust issues in cloud computing environments. Procedia Engineering,2011 15, 2852-2856.
7. Yu, S., Wang, C., Ren, K., Lou, W. Achieving secure, scalable, and fine-grained data access control in cloud computing. IEEE INFOCOM 2010.
8. Zissis, D., Lekkas, D. Addressing cloud computing security issues. Future Generation Computer Systems,2010 28(3), 583-592
9. Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W. Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 2012 ,5(2), 220-232.
10. Zhang, R., Liu, L. Security models and requirements for healthcare application clouds. IEEE Cloud 2010, 268- 275.