iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67187

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Secure WebCloud: Enforcing Security Contracts in Cloud Environments

CH Lalith Kumar[1], K Shreyas Reddy[2], Dr. M. Shanthi Thangam[3]
[1, 2]*UG Scholar, Department of CSE with Cyber Security, Sathyabama University, Chennai, India*
[3]*Associate Professor, M.E., Ph.D, Sathyabama University, Chennai, India*

Abstract: ***SecureWebCloud presents a novel approach to addressing security concerns in cloud environments through the enforcement of security contracts. As cloud computing becomes increasingly ubiquitous, ensuring the confidentiality, integrity, and availability of data and services becomes paramount. However, traditional security mechanisms often fall short in dynamically changing and multi-tenant cloud environments. SecureWebCloud proposes a proactive solution by formalizing security requirements into contracts that are enforced at runtime. Leveraging a combination of policy-based enforcement and runtime monitoring, SecureWebCloud ensures that security policies are consistently applied across diverse cloud infrastructures. These abstract highlights the key components and benefits of SecureWebCloud, positioning it as a promising avenue for enhancing security in cloud computing. By integrating with existing cloud service providers and offering a seamless interface for defining and monitoring security policies, Secure Web Cloud aims to enhance the overall security posture of organizations, reduce the risk of data breaches, and ensure compliance with regulatory requirements. The project will also focus on scalability and performance, ensuring that the security enforcement mechanisms do not impede the operational efficiency of cloud services. Through comprehensive testing and validation in real-world scenarios, Secure Web Cloud aims to provide a reliable and effective solution for enforcing security contracts in cloud environments. This abstract highlight the key components and benefits of Secure Web Cloud, positioning it as a promising avenue for enhancing security in cloud computing. The rapid adoption of cloud computing has revolutionized the way organizations deploy and manage their IT resources. However, the shift to cloud environments also introduces significant security challenges, particularly in enforcing consistent security policies across diverse and dynamic cloud services. The Secure Web Cloud project aims to address these challenges by developing a robust framework for enforcing security contracts in cloud environments. This framework will leverage advanced cryptographic techniques, machine learning algorithms, and automated policy management to ensure that security requirements are consistently met, regardless of the underlying cloud infrastructure.***

Keywords: SecureWebCloud, Scalability, Security, Reliable, Data Breaches, Security Policies.

I. INTRODUCTION

In the rapidly evolving landscape of cloud computing, ensuring robust security measures has emerged as a paramount concern for organizations across various industries. The inherently dynamic nature of cloud environments, coupled with the proliferation of diverse applications and services, poses significant challenges for traditional security paradigms. As a result, there is a pressing need for innovative approaches that can effectively safeguard sensitive data and critical resources in the cloud. Secure WebCloud stands at the forefront of addressing these challenges by introducing a pioneering framework for enforcing security contracts within cloud environments. By encapsulating security requirements into formal contracts and dynamically enforcing them at runtime, Secure Web Cloud offers a proactive and adaptable solution to mitigate security risks in the cloud. The proliferation of cloud computing has transformed the IT landscape, offering unprecedented scalability, flexibility, and cost-efficiency. Organizations across various sectors are rapidly adopting cloud services to meet their ever-growing computational and storage needs. However, this shift to cloud environments brings forth significant security challenges, as sensitive data and critical applications are now hosted on external infrastructure. Ensuring robust security measures and compliance with regulatory standards in such a dynamic and diverse environment is a daunting task. The Secure Web Cloud aims to address these challenges by developing an advanced framework for complex and evolving nature of cloud services. By leveraging cutting-edge cryptographic techniques, machine learning algorithms, and automated policy management tools, Secure Web Cloud ensures that security policies are consistently applied, monitored, and updated across all cloud platforms. A key aspect of Secure Web Cloud is its seamless integration with existing cloud service providers. This integration enables organizations to define and enforce security policies without disrupting their current operations.

In addition to enhancing security, Secure Web Cloud aims to assist organizations in achieving and maintaining compliance with various regulatory requirements such as GDPR, HIPAA, and PCI-DSS. The framework includes comprehensive logging, monitoring, and reporting capabilities that facilitate audit processes and ensure transparency. Through rigorous testing and validation in real-world scenarios, Secure Web Cloud aspires to deliver a reliable and effective solution for enforcing security contracts in cloud environments. By doingso, the seeks to significantly improve the overall security posture of organizations, reduce the risk of data breaches, and build trust in cloud computing as a secure and viable option for modern enterprises. SecureWebCloud standsat the forefront of addressing these challenges by introducinga pioneering framework for enforcing security contracts within cloud environments. By encapsulating security requirements into formal contracts and dynamically enforcing them at runtime, SecureWebCloud offers a proactive and adaptable solution to mitigate security risks in the cloud. This aims to develop advanced methodologies and tools that can automatically and dynamically enforce security contracts in real-time, ensuring that cloud resources are secure, compliant, and resilient against a wide array of cyberthreats. By leveraging cutting-edge technologies such as machine learning, blockchain, and privacy-preserving techniques, SecureWebCloud seeks to create a more secure and trustworthy cloud environment. The also addresses the need for interoperability across multi-cloud andhybrid cloud deployments, ensuring that security contracts can be uniformly applied regardless of the underlying infrastructure. Through this research, SecureWebCloud aspires to provide organizations with the confidence to fully leverage the benefits of cloud computing while mitigating the risks associated with security breaches, data privacy issues, and regulatory non-compliance. As organizations increasingly migrate their operations to the cloud, ensuring the security of sensitive data and maintaining compliance with regulatory standards have become paramount concerns. Security contracts, which define the rules and policies governing data protection, access control, and compliance in cloud environments, serve as a foundational element in safeguarding cloud infrastructures. However, the dynamic, multi-tenant nature of cloud services, coupled with the diverse and evolving threat landscape, presents significant challenges in enforcing these contracts consistently and effectively across different platforms.

II. LITERATURE REVIEW

There are plenty of researchers who have worked hard to produce a secure web cloud by enforcing security contracts in cloud environments. By ensuring scalability, security and encryption standards.

"Big Data Security and Privacy Issues in Cloud Computing: A Comprehensive Survey" (2015) by Chen et.: This survey paper provides a comprehensive overview of security and privacy issues in big data cloudcomputing. It covers various aspects, including data privacy, access control, encryption, and secure data transfer. The study emphasizes the importance of integrating security mechanisms in big data cloud environments

"Securing Big Data in the Cloud: Challenges and Countermeasures" (2017) by Goyal.: This researchexamines the security challenges of big data in the cloud and proposes countermeasures to address them.It discusses the use of encryption, data masking, and secure data transfer to protect sensitive information. The study highlights the need for multi-tenancy security to mitigate risks associated with shared cloud resources. on rare attacks.

"Privacy-Preserving Big Data Analytics in Cloud: Review and Open Challenges" (2018) by Wang.: This review paper focuses on privacy-preserving techniques for big data analytics in the cloud. It explores privacy-preserving data mining, secure multiparty computation, and homomorphic encryption as methods to ensure data privacy. The research discusses open challenges and future directions for secure big data analytics in the cloud.

"Data Security in Cloud Computing: A Comprehensive Survey" (2019) by Kaur.: This comprehensive survey covers various aspects of data security in cloud computing, including big data security. It discusses access controls, Identity and Access Management (IAM), and data classification as critical components of data security. The study emphasizes the importance of data governance and compliance in securing big data in the cloud.

"A Survey of Big Data Security Management in Cloud Computing" (2020) by Sharma.: This survey explores big data security management in cloud computing, with a focus on access control mechanisms and threat detection. It discusses the role of real-time monitoring and anomaly detection in identifying security incidents. The study highlights the importance of incident response and recovery in ensuring data confidentiality and integrity.

"Enhancing Big Data Security and Privacy in Cloud Computing Environments: A Review" (2021) by Almorsy.: This review paper discusses various security and privacy challenges in big data cloud computing protect sensitive data. The research also explores the impact of cloud service models on big data security andprivacy.

The related work for the SecureWebCloud , focused on enforcing security contracts in cloud environments, spans several key areas of research, including cloud security frameworks, policy enforcementmechanisms, privacy-preserving technologies, and compliance management in cloud computing.

Blockchain for Security and Compliance: Research has explored the use of blockchain technology to enforce security policies and compliance in cloud environments. Projects like *Hyperledger* have shown how blockchain can create immutable audit trails and decentralized trust mechanisms, which are highly relevant to enforcing and verifying security contracts in the cloud.

Cross-Cloud and Hybrid Cloud Security: Research in cross-cloud and hybrid cloud security focuses on creating standards and protocols that enable consistent security enforcement across multiple cloud platforms. Efforts like the IEEE Intercloud Working Group aim to establish such standards, which are crucial for ensuring that security contracts are enforceable across diverse cloud environments. This concept involves managing identities and access across multiple cloud services, allowing for the enforcement of consistent security policies. The research here is relevant to how security contracts can be applied uniformly across different cloud environments.

User-Centric Security Models: Research on decentralized identity management systems has explored how users can maintain control over their digital identities across cloud services. This approach aligns with the goal of giving users more control over the security contracts that govern their data. Tools and techniques that empower users to protect their privacy while interacting with cloud services, such as encryption tools and privacy dashboards, are also related to the user-centric aspects of enforcing security contracts.

Privacy-Preserving Technologies: Research in these areas has focused on enabling computation on encrypted data without revealing the data itself. These technologies are crucial for enforcing security contracts that require data privacy, even when data is being processed in the cloud. This technique has been explored as a way to add privacy protections to data sets shared in cloud environments. By injecting noise into data queries, differential privacy ensures that individual data points cannot be easily identified, aligning with privacy requirements in security contracts.

Cloud Security Frameworks: The National Institute of Standards and Technology (NIST) has developed a security reference architecture that outlines the components and processes necessary to secure cloud environments. This framework serves as a foundational guide for developing security policies and enforcing security controls across cloud services. The CSA provides extensive guidelines and best practices for securing cloud environments, particularly focusing on the shared responsibility model between cloud service providers and customers. The CSA's research on security frameworks like the Cloud Controls Matrix (CCM) has been influential in shaping how organizations approach cloud security contracts.

The Challenges faced in the present available web cloud are: 1) Lack of Integration: Security tools and policies are often siloed across different CSPs and third-party solutions. 2) Manual Processes: Many security processes, including policy management, monitoring, and compliance auditing, rely on manual effort. 3) Inefficient Threat Detection: Existing systems often lack advanced threat detection capabilities, relying on basic rule-based systems. 4) Complexity and Scalability: Managing security across multiple cloud platforms is complex and requires significant effort.

III. PROPOSED SYSTEM

The Methodology section describes about various works done SecureWebCloud. There is a brief description of all the methodologies that are implemented to develop a Web Cloud using cryptographic algorithms. Those proposed systems are classified based on the tools utilized and also by the implementation of the system based on architecture of the system.

A. Functional Model

Spiral model is a combination of both, iterative model and one of the SDLC model. It can be seen as if you choose one SDLC model and combine it with cyclic process. This model considers risk, which often goes un-noticed by most other models. The model starts with determining objectives and constraints of the software at the start of one iteration. Next phase is of prototyping the software. This includes risk analysis. Then one standard SDLC model is used to build the software. In the fourth phase of the plan of next iteration is prepared.

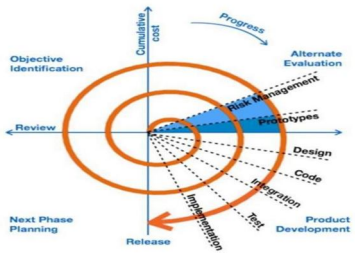


Fig1. Functional Model

After significant research on the existing systems, It comes to a conclusion that there are few drawbacks in these techniques. The claimed drawbacks are mentioned below:

Existing Techniques	Drawbacks
1) Web based Encryption 2) Attributebased Encryption	1) High ComputationalOverhead 2) Inefficient DataEncryption 3) Robust and Immediate User Revocation 4) Outsourced Decryption

Client-side encryption (CSE) is a robust method for securingdata shared in cloud platforms by encrypting data on the client's device before it is uploaded to the cloud. This approach ensures that the encryption keys remain solely in the possession of the client, providing exclusive control over dataaccess and significantly enhancing data privacy and security.With CSE, data remains encrypted during both transmission and storage, mitigating risks even if the cloud provider's infrastructure is compromised. Key management, often handled locally or via hardware security modules (HSMs), is crucial to maintaining the integrity and confidentiality of the encryption keys. Although introduces complexities in key management and potential performance overhead due to encryption and decryption processes, its benefits in protecting against unauthorized access and data breaches make it an essential strategy for organizations handling sensitive information. By implementing client-side encryption, organizations can ensure compliance with regulatory standards and maintain a higher level of data security and privacy in their cloud operations. With the increasing relianceon cloud platforms for data storage and sharing, ensuring data security has become a paramount concern. Traditional server- side encryption methods, where the cloud service provider manages encryption keys, have inherent risks, including potential access by unauthorized parties. Client-side encryption (CSE) offers a robust solution by encrypting data on the client's side before it is uploaded to the cloud, ensuringthat only the client holds the decryption keys. This approach provides enhanced security for data sharing in cloud environments. Client-side encryption provides a robust solution for secure data sharing in cloud environments by ensuring that data remains encrypted during transmission and storage and by giving users control over encryption keys. While it introduces complexities in key management and potential performance overhead, the enhanced security and privacy benefits make it a valuable approach for protecting sensitive data in the cloud. By implementing client-side encryption, organizations can mitigate risks associated with unauthorized access and data breaches, thereby safeguardingtheir critical information assets.

In this section, the system model, threat model, security requirements, and notations of MRSF are presented respectively. System Model In this paper, we consider a cloud storage system that supports ranked document retrieval in a privacy-preserving way, we consider three basic entities in our system model, namely the data owner, the cloud server, and the data user.

The data owner: ought to submit his/her encrypted data documents to the cloud server. Before data outsourcing, the data owner first builds encrypted searchable indexes for all data documents, then sends both indexes and encrypted documents to the cloud. Besides, the data owner decides the access roles for different data users. The cloud server: which has exceptional computation power and huge storage capacities, provides data hosting and processing services for data owners and data users. Upon receiving the token from an authorized data user, the cloud server first conducts search operations based on encrypted indexes and token, then returns the relevant encrypted documents. The data user: acquires the secret keys and the access roles from the data owner through a secure channel after issuing a search request. Next, the data user generates his/her search token with the secret key, then sends it to the cloud server. The secret key is also used for decrypting the retrieved resultsoff-line. Moreover, the polynomial based access control mechanism is employed to manage the decryption capabilities of data users.

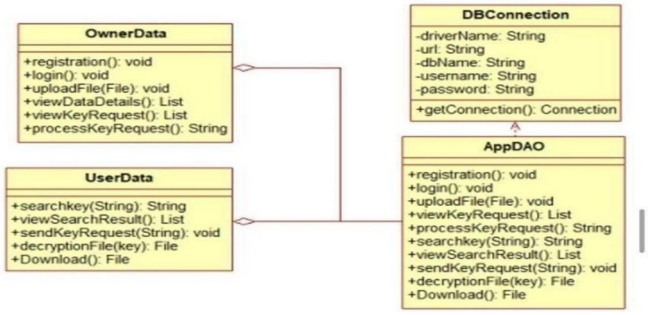


Fig2. Class Diagram

The client-side encryption for secure data sharing in cloud platforms comprises several key modules and a detailed workflow designed to enhance data security. The Encryption Algorithm Module employs AES for symmetric encryption of data and RSA for asymmetric encryption of the AES keys, ensuring robust data protection. The Key Management System (KMS) includes local key storage on the client's device and optional. The requirements that the end user specifically demands as basic facilities that the system should offer. All these functionalities need to be necessarily incorporated into the system as a part of the contract. These are represented or stated in the form of input to be given to the system, the operation performed and the output expected. They are basically the requirements stated by the user which one can see directly in the final product, unlike the non-functional requirements.

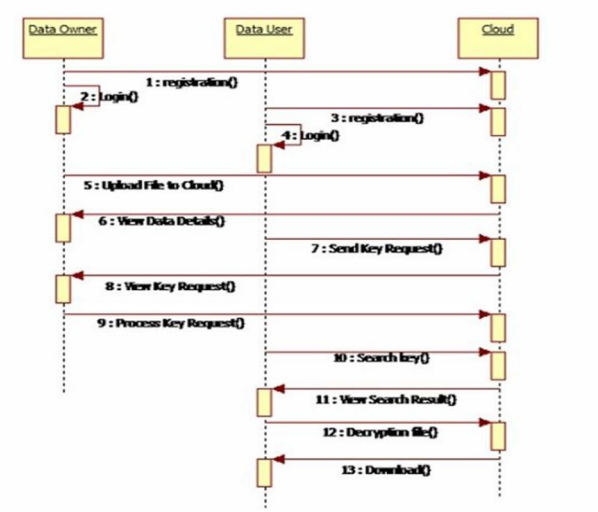


Fig3. Sequence Diagram

Hardware Security Modules (HSMs) for secure key generation and management, providing exclusive control over encryption keys. The Client Application features an encryption/decryption module that handles data encryption before upload and decryption after download, a user interface for managing encryption settings and key management, and a key exchange module for securely sharing symmetric keys. The Cloud Storage Integration ensures that only encrypted data is stored in the cloud, with secure API integration facilitating the upload anddownload processes. The workflow begins with the client application encrypting data using AES on the user's device, followed by encrypting the AES key with the recipient's public RSA key. The encrypted data and AES key are then uploaded to the cloud storage. For data sharing, the AES keyis securely sent to the recipient, who uses their private RSA key to decrypt it. The recipient then downloads the encrypteddata from the cloud and decrypts it using the decrypted AES key, allowing access to the secure data.

1) Security Contract Formalization: Developing methodologies for formalizing security requirements into contractual agreements that specify the desired security properties, constraints, and obligations.
2) Contract Lifecycle Management: Establishing mechanisms for managing the lifecycle of security contracts,including creation, negotiation, amendment, and termination,to ensure ongoing compliance with evolving security needs.
3) Policy-based Enforcement: Implementing policyenforcement mechanisms that enable the translation of security contracts into actionable policies for runtime enforcement across cloud infrastructures.
4) Runtime Monitoring and Enforcement: Integrating runtime monitoring capabilities to continuously assess and enforce compliance with security contracts, detecting and mitigating security violations in real-time.

User-visible aspects of the system that are not directly related with the functional behavior of the system. Non-Functional requirements include quantitative constraints, such as response time (i.e. how fast the system reacts to user commands.) or accuracy (.e. how precise are the systems numerical answers.) The non functionsal aspects are portability, reliability, usability, time constraints, error messages, responsive design should be implemented, space constraints, performance, standards, ethics, interoperability, security, privacy. An estimate says that 50% of whole software development process should be tested. Errors may ruin the software from critical level to its own removal. Software testing is done while coding by the developers and thorough testing is conducted by testing experts at various levels of code such as module testing, program testing, product testing, in-house testing and testing the product at user end. Early discovery of errors and their remedy is the key to reliable software.

Unit testing: Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

IV. RESULTS AND DISCUSSION

Future research in the SecureWebCloud could focus on enhancing the adaptability and automation of security contract enforcement in cloud environments. This includes developing advanced machine learning algorithms that can dynamically assess and adjust security policies in real-time, based on evolving threats and changes in cloud workloads. Additionally, research could explore the integration of blockchain technology to create immutable records of security contract compliance, thereby enhancing transparency and trust between cloud providers and users.

Another critical area of research is the development of standardized frameworks for security contracts that can be universally applied across different cloud platforms, reducing complexity and improving interoperability. Furthermore, as cloud environments continue to grow in scale and complexity, future research might investigate the use of AI-driven predictive analytics to anticipate potential security breaches before they occur, enabling preemptive adjustments to security contracts. Finally, research could also delve into the ethical implications of automated security enforcement, ensuring that such systems respect user privacy and autonomy while providing robust protection. One promising avenue is the development of context-aware security mechanisms that can intelligently adapt to different scenarios and user behaviors, automatically adjusting security contracts based on contextual factors such as location, device type, and the sensitivity of data being accessed. This could involve leveraging *contextual intelligence and anomaly detection* to identify unusual patterns that might indicate potential security threats, triggering automatic updates to security policies.

Another key area of research could focus on *cross-cloud andhybrid cloud security. As organizations increasingly adopt multi-cloud and hybrid cloud strategies, ensuring consistent enforcement of security contracts across diverse platforms becomes crucial. This could involve creating interoperability standards that allow security policies to be seamlessly applied across different cloud service providers, regardless of their underlying architectures.

Decentralized security models represent another frontier for future research. By exploring the use of decentralized technologies such as blockchain, the project could pioneer new ways to enforce security contracts in a distributed manner, reducing reliance on central authorities and potentially enhancing the resilience of cloud security againstcertain types of attacks. Additionally, blockchain could be used to create tamper-proof audit trails that ensure compliance with security contracts, providing organizations with greater transparency and accountability.

Research could also investigate privacy-preservingtechniques, such as homomorphic encryption or secure multi-party computation, which allow data to be processed while still encrypted, thereby maintaining privacy even when data is being actively used. This could be particularly valuable in environments where sensitive data is processed in shared or public cloud environments, offering new ways to enforce privacy-centric security contracts.

User-centric security models could also be a focus, with research exploring how to give users more control and visibility over the security contracts governing their data. This could involve developing user-friendly interfaces that allow individuals to customize their security settings, or creating *self-sovereign identity frameworks* that enable users to manage their digital identities across multiple platforms securely.

Finally, future research could explore the use of quantum- resistant cryptography to prepare for a future where quantumcomputing could potentially break traditional encryption methods. By investigating and implementing encryption techniques that are resistant to quantum attacks, the project could help ensure long-term security in cloud environments, even in the face of rapidly advancing technological threats.

Overall, the future research of the SecureWebCloud project should aim to create a more adaptive, interoperable, and user- centric framework for enforcing security contracts, while alsoanticipating and mitigating emerging security challenges.

1) Automated Security: Ensures consistent and robust security through automated enforcement of contracts.
2) Efficient Code Generation: Streamlines code generation with Django for seamless incorporation of security specifications.
3) Real-world Validation and Adaptability: Validated in real- world scenarios like OpenStack, showcasing effectiveness and adaptability across various cloud platforms.

V. CONCLUSION

In conclusion, implementing a client-side encryption system for secure data sharing in cloud platforms is a crucial step towards ensuring robust data security and privacy. This approach guarantees that sensitive data remains encrypted during transmission and storage, with encryption keys exclusively managed by the clients, thus mitigating the risks associated with unauthorized access and data breaches. Although the project entails significant initial development costs, ongoing maintenance, and overhead expenses, the benefits of enhanced data protection, regulatory compliance, and user trust far outweigh these investments. By integrating advanced encryption algorithms, efficient key management systems, and seamless cloud storage integration, organizations can safeguard their critical information assets and maintain a secure, trustworthy cloud environment for their users. This project not only addresses current security challenges but also positions organizations to better handle future threats and data protection requirements in an increasingly digital world. By allowing users to manage encryption keys directly on their devices. This approach significantly reduces the risk of data breaches and unauthorized access, as even the cloud service provider cannot decrypt the stored data without the client's keys. By using advanced encryption algorithms like AES for data encryption and RSA for key management, the system combines strong security measures with efficiency, making it suitable for a wide range of applications and industries. The detailed architecture and modular approach, encompassing encryption algorithms, key management systems, client applications, and cloud storage integration, provide a comprehensive solution that is both scalable and adaptable. The client-side encryption system not only enhances data security but also supports regulatory compliance with stringent data protection laws such as GDPR and HIPAA, ensuring that organizations meet their legal obligations while protecting sensitive information. However, the successful implementation of this project requires careful consideration of the associated costs, including development, infrastructure, maintenance, and overheads. The initial investment in developing a robust client-side encryption framework is substantial, but the long-term benefits of improved security, reduced risk, and enhanced user trust make it a worthwhile endeavor. Ongoing maintenance and support are also essential to address emerging security threats and to keep the system updated with the latest technological advancements. This work introduced a novel approach and tools – Secure Web Cloud – for proactive cloud security monitoring. Our key innovation lies in:

Model-driven approach: Utilizing models simplifies API design and streamlines security checks.

Automated contract-based verification: Enforces both functional and security requirements automatically, saving time and reducing human error.

Semi-automated solution: Assists developers and security experts in pinpointing vulnerabilities through automated checks, complementing manual efforts.

Adaptability to change: Automatically adjusts to updates in your cloud infrastructure, ensuring consistent security.

In summary, the adoption of client-side encryption for secure data sharing in cloud platforms represents a forward-thinking strategy to safeguard data in an era of increasing cyber threats. It provides a robust, user-controlled security framework that not only protects sensitive information but also instills confidence in users regarding the safety of their data in the cloud. As organizations continue to migrate to cloud based solutions, client-side encryption will play a pivotal role in ensuring data integrity, confidentiality, and compliance, ultimately contributing to a more secure and resilient digital ecosystem.

REFERENCES

[1] H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, “Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing,” IEEE Trans. Dependable Secure Comput., vol. 14, no. 6, pp. 679–692, Nov./Dec. 2017..

[2] W. He, D. Akhawe, S. Jain, E. Shi, and D. Song, “ShadowCrypt: Encrypted web applications for everyone,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2014, pp. 1028–1039.

[3] T. Hunt, “Hacked dropbox login data of 68 million users is now for sale on the dark web,” Tech. Rep., Sep. 2016. [Online]. Available:

[4] K. Korosec, “Data breach exposes trade secrets of carmakers GM, Ford, Tesla, Toyota,” TechCrunch, Tech. Rep., Jul. 2018.

[5] D. Lewis, “icloud data breach: Hacking and celebrity photos,” Duo Security, Tech.Rep.Sep.2014.

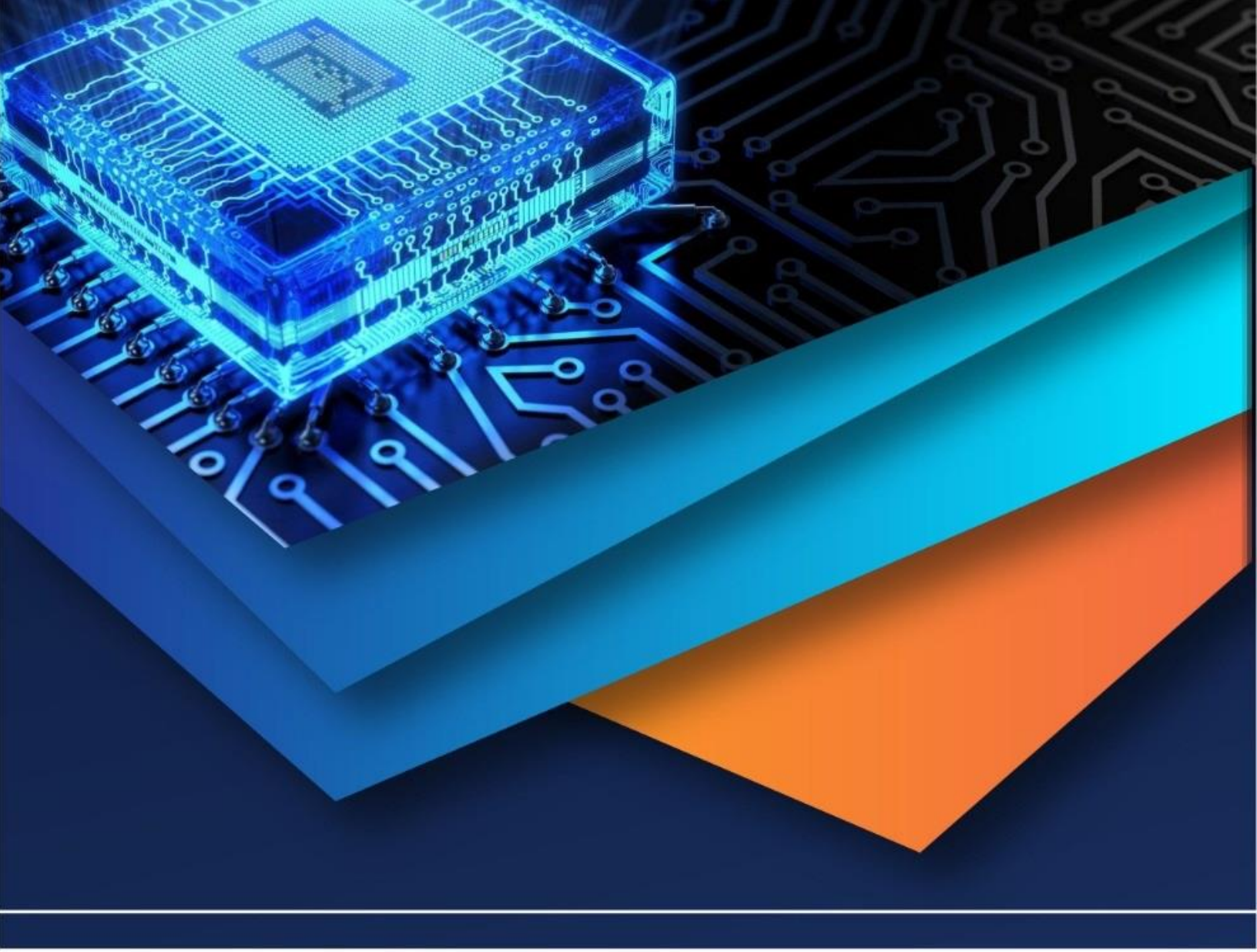
[6] W. Ma, J. Campbell, D. Tran, and D. Kleeman, “Password entropy and password quality,” in Proc. 4th Int. Conf. Netw. Syst. Secur., 2010, pp. 583– 587. Vulnearability and threat in 2018, Skybox Security, Tech. Rep., 2018

[7] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches." Wireless Communications and Mobile Computing, 13(18), 1587-1611.

[8] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data." Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS).

[9] E. Bocchi, I. Drago, and M. Mellia, “Personal cloud storage: Usage, performance and impact of terminals,” in Proc. 4th IEEE Int. Conf. Cloud Netw., 2015.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY